

Mi Primer Bitcoin ha creado esta obra y la ha puesto
disponible gratuitamente bajo **Creative Commons**.

Esta obra tiene una licencia bajo
Creative Commons
Atribución-CompartirIgual
4.0 International (CC BY-SA 4.0)

ISBN: 979-8-9993874-1-7



Diplomado de Bitcoin

Educación Financiera para la Era Bitcoin

Libro de Trabajo para Estudiantes

Versión en Español | 2025



bc1q5es60qpa7gpkp0k32xl4zefkj43kd9zjkzd54sgmv3yxr34dw8dqm9pzsd

Para donar



La Historia del Diplomado en Bitcoin

No hay nada más poderoso que una idea cuyo momento ha llegado.

La historia del Diploma Bitcoin comenzó en El Salvador, con el primer grupo de 38 estudiantes de escuelas públicas que se graduaron en junio de 2022; este fue el primer Diploma Bitcoin en un sistema escolar público en cualquier parte del mundo.

Es difícil creer que eso haya sucedido hace menos de tres años.

Desde entonces, el crecimiento ha sido fenomenal, con miles de graduados del Diploma Bitcoin de nuestras clases en todo el país. Sin embargo, el crecimiento más emocionante e inspirador ha venido de otros. El libro de ejercicios es de código abierto y una colección increíblemente diversa de educadores de Bitcoin han adoptado el material, tanto en El Salvador como en otros lugares.

El Ministerio de Educación de El Salvador lo utilizó como material fuente principal para su propio Diploma de Bitcoin y en 2024, nos unimos a Bitcoin Beach para capacitar a más de 400 maestros de escuelas públicas para enseñarlo en sus escuelas.

Uno de nuestros objetivos originales era enseñar a una nación y demostrar que la educación sobre Bitcoin es una fuerza para el bien a gran escala. Ese sueño ya está en camino.

El Salvador es el foco; la misión es el mundo.

En marzo de 2023, fundamos la red internacional de nodos de educadores de Bitcoin, que exige que todos los nodos acepten algunos principios básicos: que la educación debe ser independiente, imparcial, dirigida por la comunidad, solo en Bitcoin, de alta calidad y centrada en el empoderamiento. Esta red, que ahora es autónoma, ha traducido el trabajo a más de ocho idiomas y ha impartido el Diplomado de Bitcoin en Canadá, Estados Unidos, México, Guatemala, Honduras, Costa Rica, Cuba, República Dominicana, Haití, Colombia, Surinam, Perú, Brasil, Argentina, Irlanda, Reino Unido, Portugal, Georgia, Ghana, Nigeria, Uganda, Kenia, Zambia, Zimbabwe, Sudáfrica, Afganistán, Bangladesh, India, Hong Kong, Indonesia y Australia. La red agrega nuevos nodos cada mes y, dado que el trabajo es de código abierto, nadie necesita permiso. Es probable que muchos más lo hayan hecho completamente por su cuenta.

Este es un movimiento global y descentralizado.

La educación independiente, imparcial y dirigida por la comunidad sobre Bitcoin cambiará el mundo. Ya lo ha hecho.

Por un mundo mejor,

Equipo Mi Primer Bitcoin 2025

Tabla de Contenidos

Capítulo #1: ¿Por qué necesitamos dinero?

1.0 Introducción	01
1.1 Conoce a Satoshi	01
Actividad: 5 preguntas sobre dinero	01
1.2 Discusión en clase - ¿Por qué necesitamos el dinero?	04

Capítulo #2: ¿Qué es el Dinero?

2.0 Introducción	07
Actividad: Discusión en clase - ¿Qué es el Dinero?	07
2.1 Definición de dinero	07
2.2 Función del dinero	09
2.3 Propiedades del dinero	10
2.4 Tipos de dinero	13
2.5 Psicología del dinero: escasez, preferencia temporal y compensaciones	14
Actividad: Preferencia temporal	16

Capítulo #3: La Historia del Dinero

3.0 Introducción	21
Actividad: Juego de trueque	21
3.1 Evolución del trueque a la moneda moderna	23
3.1.1 Problemas con las formas tempranas de dinero	23
3.1.2 Desarrollo de la acuñación y el papel moneda	24
3.1.3 Transición de dinero sonante a dinero no sonante	25
3.1.4 De papel a plástico	27
3.2 Moneda Digital	28

Capítulo #4: ¿Qué es el Dinero Fiat y Quién lo Controla?

4.0 Introducción	31
4.1 Breve historia del dinero Fiat	31
4.2 El Sistema Fiat	34
4.2.1 Un sistema monetario por decreto	34

4.2.2 Banca de reserva fraccionaria un sistema alimentado por deuda	35
Actividad: Banca de reserva fraccionaria	38
4.2.3 ¿Quién controla el sistema Fiat y cómo se benefician?	39
4.3 Monedas Digitales de Banco Central: El futuro del dinero Fiat	41

Capítulo #5: Cómo Los Problemas Conducen a Soluciones

5.0 Introducción al problema	45
5.1 Disminución del Poder Adquisitivo	45
5.1.1 Inflación monetaria y su efecto en el poder adquisitivo	45
Actividad: Los efectos de la inflación - Una Actividad de Subasta	46
5.2 La Carga Global de Deuda y la Desigualdad Social	47
5.2.1 Impacto en el individuo — Pérdida de poder adquisitivo	47
5.2.2 Impacto en la sociedad — Aumento de la desigualdad de riqueza	52
Actividad: Consecuencias del sistema Fiat	53
5.2.3 La carga global de deuda	54
5.3 Los Cypherpunks y la búsqueda de una moneda descentralizada	55
5.3.1 Los Cypherpunks	56
5.3.2 Sistemas centralizados vs. descentralizados	57
5.3.3 Breve historia de las moneda digitales	59

Capítulo #6: Una Introducción a Bitcoin

6.0 Satoshi Nakamoto y la creación de Bitcoin	63
6.1 ¿Cómo funciona Bitcoin?	65
6.1.1 El mecanismo de consenso de Nakamoto	65
6.1.2 Los jugadores del juego	67
Actividad: Construcción de consenso en una red Peer-to-Peer	69
6.2 Bitcoin como dinero digital sólido	71
6.2.1 Introducción	71
6.2.2 Características de Bitcoin	72
Actividad: Discusión en clase — ¿Es Bitcoin dinero sólido?	76
6.2.3 Aceptando la responsabilidad personal	76

Capítulo #7: Cómo Utilizar Bitcoin

7.0 Introducción	81
7.1 Adquisición e intercambio de Bitcoin	81
7.1.1 P2P: físico	81
7.1.2 Intercambios P2P: en línea	82
7.1.3 Plataformas de intercambios centralizado	82
7.2 Una introducción a las carteras de Bitcoin	83
7.2.1 Carteras auto custodiadas vs custodiadas por terceros	83
7.2.2 Diferentes tipos de carteras de Bitcoin	85
7.3.3 Código abierto vs código cerrado	86
Actividad: Evaluación en clase de las carteras de Bitcoin	87
7.3 Configuración de una cartera de Bitcoin móvil	87
Actividad: Configuración/recuperación de una cartera de Bitcoin	87
7.4 Recepción y envío de transacciones	89
Actividad: Transacciones de Bitcoin en acción	91
7.5 Ahorro en Bitcoin	93
7.6 No confíes, verifica	94

Capítulo #8: La Red de Lightning: Utilizando Bitcoin en tu Vida Diaria

8.0 Introducción	97
Actividad: Ver "Bitcoin Lightning Network Explicado: Cómo Funciona en Realidad"	98
8.1 La Red Lightning	98
8.2 Diferentes tipos de Billeteras Lightning	100
8.2.1 Billeteras de autocustodia vs. Billeteras de custodia	100
8.2.2 Código abierto vs. código cerrado	100
8.3 Configuración de una Billetera Bitcoin Lightning	100
8.4 Envío y recepción de transacciones Lightning	102
Actividad: Carrera de relevos con Billeteras Lightning	106
8.5 Comprar café y comestibles con Bitcoin	107
8.5.1 En línea: Plugins de pago — comercio electrónico	108
8.5.2 En persona: Encontrar un comerciante en tu área	109
8.5.3 Herramientas de transición: Tarjetas de regalo y tarjetas de pago	110
8.5.4 Economías Circulares y Bitcoin como medio de intercambio	110

Capítulo #9: Una Introducción al Aspecto Técnico de Bitcoin

9.0 Introducción	115
Actividad: Ver "Cómo funciona Bitcoin bajo el capó"	115
9.1 Claves públicas y privadas: Seguridad a través de la criptografía	116
9.1.1 Criptografía claves públicas/privadas	116
9.1.2 Explicación del Hashing	119
Actividad: Generar Hash SHA-256	121
9.2 El modelo UTXO	122
9.3 Nodos y mineros de Bitcoin	125
9.3.1 ¿Qué es un nodo de Bitcoin y cómo configuro uno?	125
Actividad: Ver video sobre nodos de Bitcoin	126
9.3.2 ¿Qué es un minero de Bitcoin y cómo funciona la minería?	126
9.4 ¿Qué es el Mempool?	132
Actividad: Mempool	134
9.5 Cómo funcionan las transacciones de bitcoin de principio a fin	135

Capítulo #10: ¿Por qué Bitcoin?

10.0 Introducción	139
Actividad: ¿Cómo podría ser el futuro con Bitcoin?	139
10.1 ¿Qué son las Monedas Digitales de Banco Central (CBDC) y quién las controla?	140
10.2 La Filosofía de Bitcoin	141
Actividad: Discusión en clase — ¿Tienes derecho a controlar tu propio dinero?	141
10.3 Los beneficios de Bitcoin	142
10.4 Un futuro empoderado	143
Actividad: Discusión en clase — ¿Cómo cambió tu perspectiva?	143
Recursos adicionales	147
Conceptos clave del capítulo	149
Glosario	153

Diplomado de Bitcoin

*Un Viaje Transformador de Diez Semanas
a través de Educación Independiente, Imparcial,
de Alta Calidad y Gratuita*

Es esencial tener un sólido conocimiento de los conceptos básicos del dinero, su historia y el sistema financiero actual antes de estudiar Bitcoin. Comprender estos conceptos proporciona una base sólida para comprender la naturaleza única y disruptiva de Bitcoin. Al aprender sobre la evolución del dinero, podrás entender mejor el potencial y las limitaciones del sistema financiero actual y cómo Bitcoin pretende abordarlos. Sin esta base, podría ser difícil apreciar completamente la importancia y el impacto potencial de Bitcoin. Confía en el proceso de aprendizaje y mantén el enfoque, ya que la recompensa de una comprensión más profunda y aprecio de este campo de vanguardia valdrá la pena.

Capítulo #1

¿Por qué necesitamos dinero?

1.0 Introducción

1.1 Conoce a Satoshi

Actividad: 5 preguntas sobre dinero

1.2 Discusión en clase — ¿Por qué necesitamos dinero?

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

¿Por qué necesitamos dinero?

1.0 Introducción



El dinero es uno de los mayores instrumentos de libertad jamás inventados por el hombre.

Friedrich Hayek

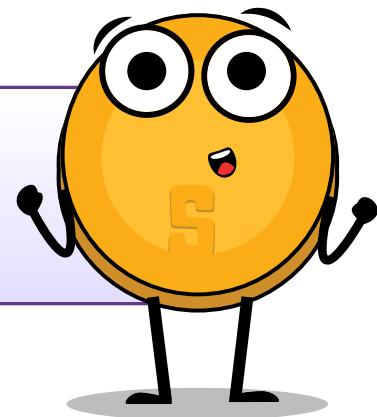


Bienvenido al Diplomado en Bitcoin. En este capítulo, exploraremos la pregunta fundamental de por qué el dinero es esencial en nuestras vidas. Analizaremos la naturaleza del dinero y sus diversas formas, con el objetivo de obtener una comprensión más profunda de su importancia. El dinero es algo que usamos casi todos los días, pero ¿realmente entendemos por qué lo necesitamos y qué es? ¿Por qué nuestros padres y otros familiares intercambian su tiempo por dinero? ¿Por qué algunas personas tienen más que otras? ¿Por qué el dinero es diferente en otros países? ¿Por qué no podemos simplemente crear más cuando lo necesitamos?

1.1 Conoce a Satoshi



¡Hola! Soy Satoshi, un asistente interactivo que te ayudará a lo largo del Diploma de Bitcoin. Te proporcionaré recursos y recomendaciones útiles para que puedas examinar de cerca conceptos clave.



Actividad: Comencemos el capítulo respondiendo las 5 preguntas a continuación:

Considera usos prácticos como adquirir necesidades como alimentos y objetos deseados. Intenta ser específico en tus ejemplos, equilibrando creatividad con el realismo.

Capítulo #1

¿Por qué necesitamos dinero?

¿Qué es el dinero?

¿Por qué necesitamos dinero?

¿Quién controla el dinero?

¿Qué le da "valor" al dinero?

Capítulo #1

¿Qué pregunta tienes sobre el dinero? Escribe tu pregunta aquí para compartirla con la clase.

Amplía la discusión a toda la clase, compartiendo y comparando listas para determinar las cinco razones más esenciales para necesitar dinero. Identifica ideas comunes en toda la clase. Reflexiona sobre tus ideas únicas que no aparecieron en la lista pero que vale la pena considerar. Anota estas ideas adicionales.

1.2 Discusión en clase — ¿Por qué necesitamos dinero?

La clase se dividirá en grupos y:

- ◆ Compartirán y discutirán las respuestas de las primeras 4 preguntas. Escriban las respuestas favoritas.
- ◆ Compartirán su respuesta a la última pregunta, voten por la pregunta favorita formulada por alguno de los estudiantes.
- ◆ La clase volverá a visitar sus respuestas y preguntas al finalizar el Diplomado en Bitcoin.

Ahora que tienes una comprensión más clara de por qué es necesario el dinero, los próximos capítulos explorarán qué es el dinero, cómo evolucionó a lo largo del tiempo, quién lo influye y la forma más reciente de dinero. Sigue consultando tus listas de este primer día en clase para establecer conexiones entre tus percepciones y la evolución de la creación, definición y uso del dinero a lo largo del tiempo.

Capítulo #2

¿Qué es el dinero?

2.0 Introducción

Actividad: Discusión en clase — ¿Qué es el Dinero?

2.1 Definición de Dinero

2.2 Función del dinero

2.3 Propiedades del dinero

2.4 Tipos de dinero

2.5 Psicología del dinero: escasez, preferencia temporal y compensaciones

Actividad - Preferencia Temporal

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

¿Qué es el Dinero?

2.0 Introducción



El dinero es una garantía de que podremos tener lo que queremos en el futuro. Aunque no necesitemos nada en este momento, asegura la posibilidad de satisfacer un nuevo deseo cuando surja.

Aristóteles



Continuando con nuestra exploración de la necesidad del dinero, este capítulo aborda la pregunta central: ¿Qué es el dinero? Comenzaremos con una discusión grupal y una actividad.

Actividad - Discusión en Clase — ¿Qué es el Dinero?

- 💡 Por favor, no coman el caramelo colocado en sus escritorios aún.
- 💡 ¿Quién estaría dispuesto a intercambiar su caramelo por un billete de \$1?
- 💡 Ahora, mantengan las manos arriba si aún estarían dispuestos a cambiar su caramelo por un billete de \$1 de monopoly?
- 💡 ¿Por qué sí o por qué no?
- 💡 ¿Qué hace que un billete sea tan deseable y otro tan bueno como basura?
- 💡 ¿Qué le da "valor" al dinero?
- 💡 ¿De dónde proviene el dinero, y quién decide cuánto imprimir?
- 💡 ¿Por qué no imprimir más dinero y distribuirlo equitativamente entre todos?

La única diferencia entre estas dos notas es tu creencia de que una tiene más valor que la otra.



2.1 Definición de Dinero

¿Alguna vez te has detenido a pensar en qué es realmente el dinero? ¿Te has preguntado qué hace que el dinero sea... dinero? La mayoría de nosotros sabe cómo usarlo, pero pocos comprenden de dónde proviene o cómo funciona. El dinero es esencialmente una forma de intercambiar bienes y servicios. Representa el valor de estos elementos en una forma que puede intercambiarse fácilmente. Esto puede adoptar muchas formas diferentes, como billetes de papel, monedas metálicas y pagos electrónicos. Normalmente, los gobiernos u otras autoridades emiten y controlan el dinero. Pero el dinero es mucho más que simplemente un medio de intercambio físico o digital. Es como un lenguaje universal que nos permite comerciar con personas de todo el mundo, incluso si no hablamos el mismo idioma o compartimos la misma cultura. Por ejemplo, puedes estar en el otro lado del mundo y aún "hablar" dinero, al colocar un producto en el mostrador y cambiarlo por la moneda local o al usar una tarjeta de crédito.

Capítulo #2

El dinero es como un contrato social que nos permite realizar intercambios sin tener que depender del trueque o encontrar a alguien que específicamente quiera lo que tenemos para ofrecer. Si un grupo de personas comenzaría a aceptar chocolate como pago por la mayoría de los bienes y servicios, el chocolate se convertiría en dinero. (Aunque, dado que se derretiría en algunas partes del mundo, podríamos considerarlo un mal dinero).

Como señaló el economista francés Jean Baptiste Say: "El dinero realiza solo una función momentánea en un intercambio; y cuando la transacción se cierra finalmente, siempre se encontrará que se ha intercambiado un tipo de mercancía por otra".

En otras palabras, el dinero en sí mismo no tiene el poder de satisfacer los deseos humanos. Es simplemente una herramienta que nos permite intercambiar una mercancía por otra.



Transacción es un intercambio o transferencia de bienes y servicios. Es una forma de intercambiar valor entre dos o más partes.

Hay muchos tipos diferentes de transacciones, que van desde intercambios simples (como comprar un sándwich en una tienda de delicatessen) hasta transacciones financieras más complejas (como comprar una casa o invertir en acciones o bonos). Las transacciones pueden realizarse en persona, por teléfono, en línea o por otros medios, y pueden involucrar a una amplia gama de partes, incluidos individuos, empresas e instituciones financieras.



Mira este
vídeo corto!



Sin dinero, ¿Qué tan fácil sería este intercambio?

¿Cambiarías una vaca por 1 million de fresas?

¿O es 600,000 fresas? ¿Qué tal 50,000?



El dinero **ES** el valor **mediante** el cual se intercambian bienes y servicios. El dinero **NO ES** el valor **POR** el cual se intercambian bienes.

En resumen, el dinero:

facilita el comercio porque todos lo aceptan como pago final. Nos permite medir el valor y comparar diferentes bienes y servicios. A continuación, analizaremos la función del dinero.

¿Qué es el Dinero?

2.2 Función del dinero

Cuando se trata de comprar y vender bienes y servicios, el dinero es el jugador clave. El dinero cumple varias funciones importantes en el mundo, como:

1

Reserva de valor

El dinero debe mantener su valor con el tiempo, lo que lo hace útil como una forma de ahorrar e invertir el valor del trabajo humano. Esto permite a las personas utilizar el dinero para planificar el futuro y para pedir prestado y prestar dinero. Así que la próxima vez que estés ahorrando para algo especial, recuerda que el dinero es más que solo una forma de pagar cosas, es una herramienta que te ayuda a planificar e invertir en tu futuro.

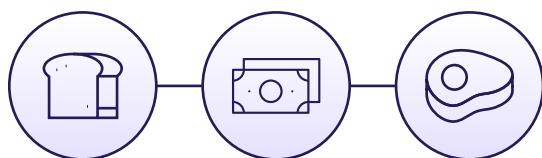
¿Cuál es tu reserva de valor?	BTC (USD)	Oro (USD)	USD (EUR)
Marzo 14, 2019	\$3,846	\$1,293	€0.8817
Marzo 14, 2020	\$5,258	\$1,529	€0.90056
Ganancia/Pérdida	+36.71%	+18.25%	+2.14%

2

Medio de intercambio

Con dinero, no tienes que encontrar a alguien que quiera exactamente lo que tienes para intercambiar. En cambio, puedes usar dinero para comprar y vender cualquier cosa que desees. Esto hace que el comercio y el intercambio sean mucho más convenientes y eficientes.

Medio de intercambio



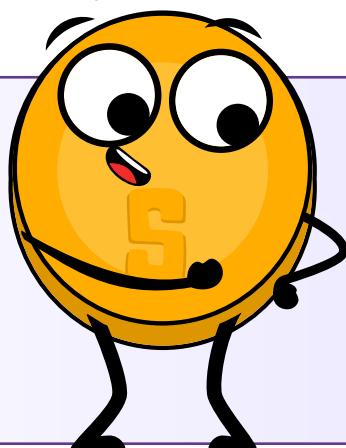
3

Unidad de cuenta

El dinero proporciona un estándar universal de valor que permite a las personas expresar y comparar el precio de diferentes bienes y servicios. Esto permite un mercado más eficiente y transparente, donde las personas pueden tomar decisiones informadas sobre qué comprar y vender.

Unidad de cuenta

Los consumidores saben el valor de algo cuando se les asigna un precio (valor monetario) a las cosas.



\$29.00

\$350.00



Piénsalo de esta manera: si quisieras comprar un carro nuevo, podrías comparar precios de diferentes concesionarios y tomar una decisión informada sobre cuál comprar basándote en el precio en dólares. Sin una unidad de cuenta, tendrías que intentar comparar el valor de un carro con otro usando algo más, como la cantidad de vacas que valía o el tiempo que tomó fabricar el carro.

Estas tres funciones son las que permiten que las economías se vuelvan complejas y dinámicas. Sin dinero, sería mucho más difícil comprar y vender bienes y servicios, y nuestra economía estaría mucho menos desarrollada.

Ejercicio en clase — ¿A qué función del dinero se refiere este ejemplo?

-  Daniel decidió ahorrar una parte de su sueldo semanal para comprar un cachorro.
-  Alex compra dos rebanadas de pizza por \$8.30 en Ray's Pizza.
-  Linda no puede decidir si comprar boletos para un concierto por \$75 o comprar un pase de esquí por \$95.

2.3 Propiedades del dinero

Con el tiempo, las personas han llegado a darse cuenta de que el dinero debe poseer ciertas cualidades para ser efectivo como medio de intercambio. Estas características incluyen durabilidad, portabilidad, divisibilidad, fungibilidad, escasez y aceptabilidad.

 **Durabilidad** se refiere a la capacidad del dinero para resistir el deterioro físico y durar con el tiempo. Esto asegura que el dinero pueda circular en la economía en un estado aceptable y reconocible. El oro es un material duradero que puede resistir el desgaste, lo que lo convierte en una buena representación de la durabilidad característica del dinero.

 **Divisibilidad** se refiere a la capacidad del dinero para dividirse en unidades más pequeñas, para que las personas puedan usarlo para realizar compras de diferentes cantidades. Los billetes de papel se pueden dividir fácilmente en denominaciones más pequeñas, lo que los convierte en una buena representación de la característica de divisibilidad del dinero.



¿Qué es el Dinero?

● **Portabilidad** se refiere a la facilidad con la que el dinero puede ser transportado y llevado consigo. Esto permite a las personas usar dinero para comprar y vender bienes y servicios sin dificultad. Las tarjetas de crédito son portátiles, ya que pueden llevarse fácilmente en una billetera o bolso, lo que las convierte en una buena representación de la característica de portabilidad del dinero.



● **Aceptabilidad** se refiere a la amplia aceptación del dinero como forma de pago, para que las personas puedan usarlo para comprar y vender bienes y servicios con confianza. El dólar estadounidense es ampliamente aceptado como forma de pago, lo que lo convierte en una buena representación de la característica de aceptabilidad del dinero.



● **Escasez** se refiere a la oferta limitada de dinero, que ayuda a mantener su valor y evita que tengamos que gastar más dinero para comprar la misma cantidad de bienes. Los sellos coleccionables, especialmente los raros y valiosos, pueden ser una buena forma de dinero porque son escasos y su valor puede aumentar con el tiempo. Los coleccionistas de sellos suelen utilizar sus sellos como una forma de invertir su riqueza y diversificar su cartera.



● **Fungibilidad** se refiere a la intercambiabilidad del dinero, de modo que una unidad de dinero equivale a otra unidad del mismo valor. El dinero debe ser uniforme. Las monedas de cobre son uniformes en tamaño y peso, lo que las convierte en una buena representación de la uniformidad característica del dinero. Un centavo es siempre un centavo.



En general, estas características hacen que el dinero sea una herramienta útil y efectiva para facilitar el comercio y el intercambio, y son esenciales para el desarrollo y la estabilidad de las economías.

Ejercicio en Clase

Diferentes activos tienen diferentes propiedades y cumplen las funciones del dinero en diversos grados. La sociedad determina en última instancia qué activo se utiliza como dinero basándose en factores como su estabilidad, escasez, divisibilidad, transferibilidad y aceptación como medio de intercambio.

Para determinar qué tan bien cumplen diferentes elementos con las características específicas del dinero, puedes calificar cada elemento en una escala del 1 al 5 para cada característica. Al sumar las puntuaciones para cada elemento, puedes determinar cuál es el más adecuado para ser una forma de dinero

[0 = Terrible; 3 = Aceptable; 5 = Excelente]

* Por favor, no llenes la columna para Bitcoin; volveremos a ella más adelante en el curso.

Utiliza las siguientes preguntas para determinar si los diferentes elementos en la tabla cumplen con las características del dinero.

-  **Durabilidad:** ¿Puede el dinero resistir el desgaste con el tiempo?
-  **Fungibilidad:** ¿Es el dinero intercambiable con otras formas de dinero?
-  **Aceptabilidad:** ¿Es el dinero ampliamente aceptado como forma de pago?
-  **Escasez:** ¿Es el dinero escaso y no demasiado abundante?
-  **Portabilidad:** ¿Puede el dinero transportarse fácilmente y usarse en diferentes ubicaciones?
-  **Divisibilidad:** ¿Puede el dinero dividirse en unidades más pequeñas para transacciones?

Características de buen dinero	 VACAS	 CIGARRILLOS	 DIAMANTES	 EUROS	 BITCOIN
Durable					
Portable					
Uniforme					
Aceptable					
Escaso					
Divisible					
Total					

¿Qué es el Dinero?

2.4 Tipos de Dinero

El dinero puede dividirse en dos categorías principales: físico y digital.

El dinero físico incluye:

- ◆ Dinero fiduciario, que son los billetes de papel y monedas emitidos por los gobiernos y aceptados como medio de intercambio.
- ◆ Dinero representativo, que representa un reclamo sobre una mercancía física.
- ◆ Dinero mercancía, que es un objeto físico que tiene un valor intrínseco y es ampliamente aceptado como medio de intercambio. Por ejemplo, oro y plata.



¡No todo el dinero es igual!



Dinero Mercancía



Objetos como esta pólvora, alguna vez sirvieron como dinero mercancía.

Dinero Representativo



Dinero representativo como este certificado de plata, podía cambiarse por plata

Dinero Fiduciario



Hoy, los billetes de la Reserva Federal son dinero fiduciario, decretado por el gobierno federal para ser una forma aceptable de pagar las deudas.

Las monedas digitales por otro lado, se pueden utilizar para transacciones en línea e incluyen monedas electrónicas, monedas estables y criptomonedas.

Las monedas electrónicas son versiones digitales del dinero normal, como dólares o euros, y pueden usarse para comprar y vender cosas en línea a través de vías de pago digitales.



Las vías de pago son la infraestructura que permite el movimiento de monedas electrónicas y otros activos digitales de un lugar a otro. Sin embargo, en el sistema financiero tradicional, siempre hay un intermediario, como un banco o institución financiera, que cobra una tarifa y tiene la autoridad para aceptar, cancelar, revertir o retrasar transacciones.

En el sistema financiero intermediado, los principales tipos de "vías de pago" digitales incluyen las redes de tarjetas, que facilitan la transferencia de fondos entre instituciones financieras y comerciantes cuando un cliente realiza una compra con una tarjeta de débito o crédito, y las billeteras digitales, que son cuentas en línea que permiten a los usuarios almacenar y gestionar sus monedas electrónicas y realizar pagos transfiriendo fondos desde su cuenta a la cuenta del destinatario.



Las Monedas Digitales de Banco Central (CBDC, por sus siglas en inglés)

Son versiones digitales de la moneda fiduciaria de un país, emitidas y respaldadas por el banco central e intermediadas por el gobierno.



Las Stablecoins (monedas estables)

Son monedas digitales diseñadas para mantener un valor estable en relación con un activo, como el dólar estadounidense.



Las Criptomonedas

Son un tipo de moneda digital. Algunas criptomonedas son descentralizadas y se rigen por reglas, mientras que otras son centralizadas y controladas por un pequeño grupo de personas.

En última instancia, una moneda que opera sin intermediarios es más eficiente y beneficiosa para la sociedad, ya que evita que unas pocas personas controlen la oferta de dinero y concentren su poder. Sin embargo, crear una moneda así que facilite transacciones seguras sin depender de la confianza entre las partes ha sido un desafío a lo largo de la historia. Para lograrlo, se debe crear una moneda que opere como internet, donde el control esté distribuido entre todos y nadie al mismo tiempo. Esto requiere el acuerdo de todas las partes, incluidas aquellas que tienen poder, para renunciar al control en favor del bien común.

2.5 La psicología del dinero: escasez, preferencia temporal y compensaciones

Imagina que estás varado en un desierto y solo te queda una botella de agua. Tienes sed y desesperación por beber, pero también sabes que necesitarás el agua para sobrevivir hasta que puedas encontrar más. Este es un ejemplo clásico de escasez; solo tienes una cantidad limitada de un recurso (agua) y debes tomar una decisión sobre cómo usarlo. En esta situación, podrías decidir racionarlo y tomar pequeños sorbos durante un período más largo, para hacer que dure tanto como sea posible.

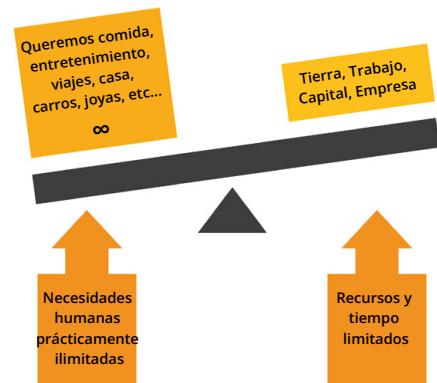
¿Qué es el Dinero?



La escasez nos obliga a sopesar los pros y los contras de cómo utilizamos nuestros recursos y hacemos concesiones.

Alternativamente, podrías decidir beber tanto como puedas de una vez, esperando que el aumento de hidratación te dé la energía que necesitas para encontrar más agua. Independientemente de la elección que hagas, te enfrentas a una decisión difícil. En este caso, la elección se trata entre saciar tu sed inmediata o conservar el agua para más tarde. Este concepto de escasez se aplica a todo tipo de recursos, no solo al agua. Ya sea dinero, tiempo o incluso amor y atención, constantemente nos enfrentamos a decisiones sobre cómo asignar nuestros recursos limitados.

Existen dos tipos de escasez: escasez creada por el humano y escasez natural.



- ◆ La escasez creada por el humano, también conocida como escasez centralizada, incluye cosas como bolsos de diseñador de edición limitada, cartas de deportes raras y piezas de arte numeradas. Estas pueden replicarse o falsificarse fácilmente.
- ◆ La escasez natural, también conocida como escasez descentralizada, incluye cosas como sal, conchas y metales preciosos como el oro. Estos son más difíciles de replicar o falsificar. La principal diferencia entre ambas es el control.

La escasez centralizada está controlada por una entidad única, como una empresa o gobierno, mientras que la escasez descentralizada no está controlada por nadie. Un ejemplo de escasez centralizada que afecta desproporcionadamente a los pobres es el control de recursos esenciales como el agua potable. En algunas regiones, el acceso al agua limpia está gestionado por empresas privadas o entidades gubernamentales que pueden limitar su distribución, provocando una escasez de este recurso vital. Este control centralizado puede resultar en aumentos de precios o un acceso desigual al agua limpia, siendo las comunidades empobrecidas a menudo las más afectadas. El acceso limitado al agua limpia no solo afecta su salud y bienestar, sino que también perpetúa la pobreza, ya que pueden verse obligadas a pagar precios más altos por el agua o viajar largas distancias para obtenerla.

La escasez afecta nuestras decisiones. Comprenderla puede mejorar nuestra toma de decisiones. A menudo, debemos elegir entre ganancias inmediatas y beneficios a largo plazo, y estos intercambios dan forma a nuestro camino hacia el logro de nuestros objetivos.



Preferencia temporal se refiere a la idea de que, en general, las personas prefieren tener algo AHORA en lugar de más tarde.



Un ejemplo de preferencia temporal:

Imagina que tienes la opción de recibir \$100 hoy o \$110 en un año. Si tienes una alta preferencia temporal, es posible que elijas recibir los \$100 hoy, porque valoras más tener los \$100 ahora que los beneficios de esperar un año para los \$10 adicionales. Por otro lado, si tienes una baja preferencia temporal, preferirás esperar la recompensa más grande, porque estás más enfocado en la planificación a largo plazo y menos preocupado por la gratificación inmediata.

Actividad - Preferencia Temporal

Alta Preferencia Temporal vs. Baja Preferencia Temporal

- 1** Escucha la explicación del maestro sobre la elección de dulces.
- 2** Decide si quieres recibir un pequeño caramelo o malvavisco ahora, o esperar hasta el final de la clase para recibir dos caramelos o un caramelo más grande y deseado.
- 3** Comprométete con tu decisión y hazle saber al maestro tu elección. Recibe tu caramelo ya sea de inmediato o al final de la clase, según tu decisión.
- 4** Participa en la discusión en clase sobre la actividad, reflexionando sobre tu proceso de toma de decisiones y el concepto de preferencia temporal.

Conclusión y Discusión:

- ?** ¿Qué factores influenciaron tu decisión de tomar el caramelo ahora o esperar una recompensa más grande después?
- ?** ¿Cómo te sientes acerca de tu decisión ahora que la actividad ha terminado?
- ?** ¿Puedes pensar en ejemplos de la vida real donde una alta preferencia temporal podría ser perjudicial y donde una baja preferencia temporal podría ser beneficiosa?
- ?** ¿Cuáles son algunas posibles consecuencias de elegir una alta preferencia temporal en lugar de una baja preferencia temporal?

En el contexto del ejemplo del desierto, esto significa que podrías estar más inclinado a beber toda el agua de inmediato, incluso si eso significa que no tendrás nada para después. Esto se debe a que la sed que sientes en este momento es más apremiante que la sed potencial que podrías sentir en el futuro.

Por otro lado, si eliges racionar el agua y beberla lentamente con el tiempo, estás demostrando una preferencia temporal más baja. Esto significa que estás dispuesto a esperar para satisfacer tu sed y mejorar tus posibilidades de supervivencia. El concepto de costo de oportunidad está estrechamente relacionado con la idea de escasez y preferencia temporal.

¿Qué es el Dinero?



El costo de oportunidad se refiere al valor de la siguiente mejor alternativa que renuncias cuando tomas una decisión. Cada decisión implica compensaciones.

La elección de hoy



Comprar un batido de fresa por \$7

Ahora



Gastar \$7 de otra manera.



Después



Beneficiarse de \$7 ahorrados regularmente

En el ejemplo del desierto, el costo de oportunidad de beber toda el agua de inmediato son los beneficios de supervivencia que habrías obtenido al racionar el agua y usarla durante un período más largo.

Imagina que decides racionar el agua y tomar pequeños sorbos durante un período más largo. Como resultado, tienes la energía e hidratación necesarias para buscar más agua. Sin embargo, mientras buscas, encuentras un cactus que tiene una pequeña cantidad de agua en su interior. No es mucho, pero es suficiente para saciar tu sed en ese momento. Si hubieras decidido beber toda tu agua de una vez, es posible que no hubieras tenido la energía para buscar más agua y encontrar el cactus.

En este caso, el costo de oportunidad de beber toda tu agua de una vez habría sido la oportunidad de encontrar el cactus y obtener más hidratación.

Este ejemplo ilustra cómo el costo de oportunidad involucra no solo la compensación inmediata entre dos opciones, sino también las oportunidades futuras potenciales que pueden ganarse o perderse como resultado de nuestras elecciones. Nuestra disposición a renunciar a una recompensa mayor en el futuro a cambio de una recompensa menor ahora está influenciada por nuestra preferencia temporal, o cuánto valoramos la gratificación inmediata frente a la planificación a largo plazo.

En este capítulo, exploramos el concepto fundamental de dinero. Este capítulo abordó la definición de dinero, sus funciones, propiedades y diversos tipos. Un aspecto esencial de nuestra discusión involucró comprender la psicología del dinero, centrándonos en conceptos como la escasez, la preferencia temporal y las compensaciones. Esta exploración sentó las bases para comprender la naturaleza complicada del dinero y su papel en nuestras vidas. En el próximo capítulo, hablaremos sobre la historia del dinero y cómo ha evolucionado a lo largo del tiempo.

Capítulo #3

La Historia del Dinero

3.0 Introducción

Actividad: Juego de trueque

3.1 Evolución del trueque a la moneda moderna

3.1.1 Problemas con las formas tempranas de dinero

3.1.2 Desarrollo de la acuñación y el papel moneda

3.1.3 Transición de Dinero Sonante a Dinero No Sonante

3.1.4 De papel a plástico

3.2 Moneda Digital

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

La Historia del Dinero

3.0 Introducción

El dinero no evolucionó por diseño, sino que surgió del proceso de mercado. No fue creado por gobiernos. Surgió con el tiempo como un orden espontáneo.

Murray Rothbard



Imagina una época en el pasado cuando la gente no tenía las monedas o billetes de papel que usamos hoy en día. En ese entonces, tenían una forma única de intercambiar cosas, usando elementos como conchas o metales preciosos como el oro como una especie de moneda especial. Puede sonar extraño, pero era su versión de dinero, algo en lo que todos estaban de acuerdo tenía valor.

En este capítulo, nos embarcaremos en un viaje a través del tiempo, experimentando de primera mano la evolución del dinero. Rastrearemos sus orígenes y observaremos cómo ha cambiado y se ha adaptado a lo largo de la historia.

Actividad: Ejercicio en clase — Juego de trueque

Tu profesor te ha dado un pequeño trozo de papel. Tu objetivo es comerciar lo que "tienes" con lo que "quieres" en un juego de comercio a lo largo de la historia. Por favor, escribe tu nombre en la parte superior del papel en letras pequeñas y legibles.

Ronda #1: Trueque

Es el año 6000 a.C. Como es de esperar, el dinero tal como lo conocemos aún no ha sido inventado. Te encuentras en Mesopotamia e intercambias bienes y servicios directamente entre ustedes a través del trueque.

Como nota adicional, muchas empresas aún aceptan pagos no monetarios por sus servicios, y los gobiernos tratan estas transacciones de trueque de la misma manera que las transacciones en moneda para fines de informes fiscales.



Corta tu hoja de papel por la línea de puntos. Tu objetivo es intercambiar tu "tener" tantas veces como sea necesario para finalmente obtener tu "querer" original. No puedes cambiar tu "querer" original. Tendrás 5 minutos para lograr el objetivo de este ejercicio.



Cuando tu nuevo "tener" coincida con tu "querer" original, regresa a tu asiento. Después de que se agote el tiempo, si no has encontrado un compañero de intercambio, regresa a tu asiento de todos modos.



Levanta la mano si lograste conseguir lo que querías después de un intercambio. ¿Dos? ¿Tres?

Responde brevemente pero de manera sustancial a las siguientes preguntas:

1. ¿Por qué algunos de ustedes pudieron encontrar a alguien con quien comerciar y otros no?

2. ¿Cuáles son los beneficios del trueque?

3. Basándote en tu experiencia con este ejercicio, ¿cuáles son las desventajas de utilizar el trueque?

💡 Ronda #2: Dinero Mercancía

Avanzamos rápidamente y viajamos a la costa oeste de África alrededor del siglo XIV a.C. El trueque se ha vuelto tedioso e ineficiente. Hemos evolucionado como civilización y ahora estamos utilizando dinero de mercancía.

Conchas de Cauri a Monedas



1300 AEC



1000 AEC



687 AEC



Hecho divertido:

Las conchas de cauri fueron aceptadas como moneda de curso legal en algunas partes de África hasta el siglo XX.

1300 AEC

Las conchas de cauri son la forma predominante de pago en la mayor parte de Asia, África, Oceanía y algunas partes de Europa.

1000 AEC

Comienza la dinastía Zhou occidental de China utilizando monedas de metal.

687 AEC

El Rey Aliados de Lidia (actual Turquía) encarga la fabricación de las primeras monedas de metal acuñadas en el mundo occidental.

Estas protomonedas tenían forma ovalada, estaban hechas de "electro" (una aleación de oro y plata) y tenían un diseño en una sola cara

La Historia del Dinero

Tu profesor te ha dado un macarrón (por simplicidad). Supongamos que, por convención, el precio de cada bien vale un macarrón.

Tu objetivo nuevamente es obtener lo que "quieres". Pero ahora, nuestra especie ha mejorado un poco y ha encontrado una manera de resolver ciertos problemas.

- 💡 ¿Por qué consideramos el macarrón como dinero de mercancía?
 - 💡 ¿Cómo obtenemos ahora las cosas que queremos?
 - 💡 ¿Fue más fácil la ronda con macarrones?
 - 💡 ¿Por qué crees que el dinero ha reemplazado a las mercancías?
 - 💡 ¿En qué formas el uso de dinero de mercancía es más eficiente que el trueque?
 - 💡 ¿Cuáles son las desventajas de usar macarrones como dinero?
 - 💡 ¿Qué crees que sucedió cuando España comenzó a traer cargamentos de macarrones a tu comunidad (oro y plata de las Américas de vuelta a España)?
-
-
-
-

3.1 Evolución desde el trueque hasta la moneda moderna

3.1.1 Problemas con las formas tempranas de dinero

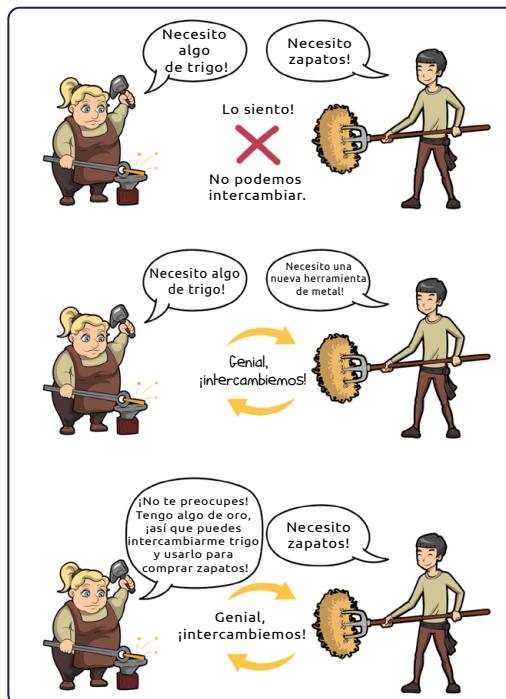


Mira este breve video para conocer los orígenes del intercambio, tiene como título: ¿Quién inventó el dinero?



En las economías de trueque, las personas intercambian entre sí basándose en el valor relativo de los bienes y servicios que tienen para ofrecer. Las economías de trueque son ineficientes y pueden ser difíciles de gestionar, especialmente en sociedades complejas.

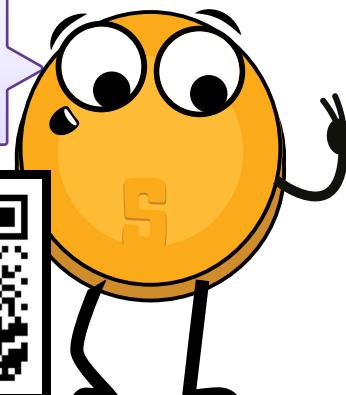
Una situación como la doble coincidencia de deseos es necesaria en cualquier sistema de trueque, ya que las personas siempre deben encontrar a alguien que tenga lo que desean, pero también desee lo que tienen para ofrecer en intercambio.



Supongamos:

- Joseph quiere intercambiar su plátano por el coco de Yael.
- Pero Yael solo quiere intercambiar su coco por el mango de Tammy.
- Y Tammy solo quiere intercambiar su mango por el plátano de Joseph.
- Están atrapados en un ciclo interminable de intercambio de frutas sin una doble coincidencia de deseos.
- Joseph sugiere que simplemente intercambien sus frutas por una soda bien fría, pero se dan cuenta de que están en una isla remota y no hay soda.
- Deciden simplemente sentarse en la playa y disfrutar de sus frutas en silencio.

**En este video
encontrarás la
"Historia del
dinero"**



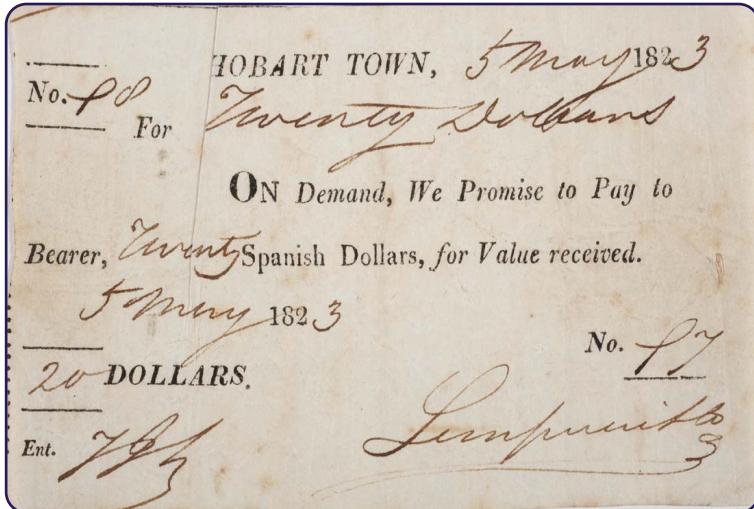
3.1.2 Desarrollo de la acuñación de monedas y el papel moneda

A medida que tú y tu comunidad se involucran más en el comercio, te das cuenta de las limitaciones del trueque y otras formas de intercambio no monetario. Decides adoptar el uso de monedas de metal como forma de dinero.



El dinero de mercancía es dinero fabricado a partir de materiales metálicos valiosos como el oro y la plata. Históricamente, se han utilizado como reserva de valor, medio de intercambio y, en el pasado lejano, como unidad de cuenta.

La Historia del Dinero



Estos recibos de papel, con sus orígenes en la antigua China, son una forma conveniente y fácilmente intercambiable de moneda. Están respaldados por oro y otros metales valiosos y se pueden convertir en estos metales durante los siglos XVII al XIX. Esto les permite tener una forma de dinero más portátil y fácilmente transferible, manteniendo al mismo tiempo el valor y la seguridad de los metales preciosos.



3.1.3 Transición de Dinero Sólido a Dinero No Sólido

Avanzamos rápidamente al siglo XVII en Suecia. Ahora dependes completamente de los bancos para almacenar tus activos valiosos. Sin embargo, comienzas a notar algo sospechoso con estos banqueros. Parece que están emitiendo más recibos de papel de los que tienen de oro almacenado, lo que les permite crear más dinero del que tienen activos para respaldarlo. Esta práctica astuta les permite a los banqueros obtener beneficios de la diferencia entre el valor de los recibos de papel y el valor del oro que están guardando para sus clientes.



¿Qué sucede cuando realmente intentas poner en práctica la doctrina del papel moneda? Descúbrelo en el video titulado "El Patrón Oro"



Te das cuenta de que esto marca un cambio importante en la forma en que funciona el dinero. Estás pasando de un sistema de dinero sonante (es decir, dinero respaldado por metales preciosos) a un sistema de dinero no sonante (es decir, moneda fiduciaria no respaldada por una mercancía física). Esta transición no ocurrió de la noche a la mañana, sino que fue un proceso gradual influenciado por varios factores. La Revolución Industrial, con su producción en masa y urbanización, desempeñó un papel, al igual que el crecimiento de sistemas financieros avanzados como bancos y mercados de valores. La aparición de bancos centrales y otras autoridades monetarias contribuyó a la centralización o control del dinero, lo que llevó a la emisión de monedas fiduciarias para respaldar el crecimiento económico.

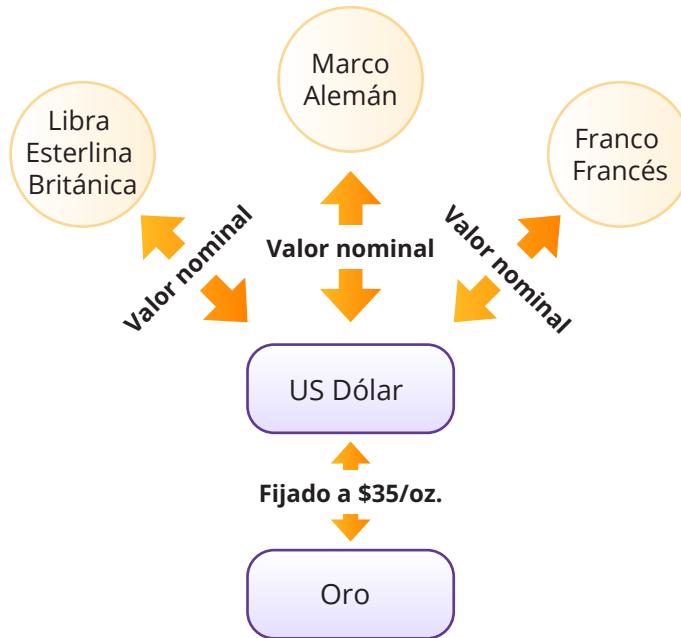


Sin embargo, también comienzas a ver los **inconvenientes de esta centralización**, que incluyen el consumo irresponsable, el **aumento de la deuda** y la manipulación de los ciudadanos a través de incentivos económicos.

Hasta la Primera Guerra Mundial, podías convertir tu dinero en papel en una cantidad preestablecida de oro. Pero las dos guerras mundiales y la crisis económica de 1929 pusieron fin a eso. En 1944, se firmó el acuerdo de Bretton Woods, estableciendo el dólar estadounidense como la moneda de reserva mundial y fijando el valor del dólar estadounidense al precio del oro a una tasa de \$35 por onza. Las monedas de otros países están vinculadas al dólar, lo que ayuda a estabilizar los mercados financieros internacionales.

Sistema Bretton Woods

(1945 — 1972)



Desafortunadamente, el sistema comenzó a desmoronarse a finales de la década de 1960, lo que llevó al Shock de Nixon en 1971, cuando el gobierno de Estados Unidos suspendió la convertibilidad del dólar en oro. Esto marca el fin del patrón oro y el comienzo de un mundo impulsado por la creación y acumulación de deuda.

Mientras llevas a cabo tu vida diaria, comienzas a notar que el valor del dinero ya no es tan estable como solía ser. Al igual que una regla flexible dificulta medir con precisión la longitud de una mesa, vivir en un mundo fiduciario donde el valor del dinero está sujeto a la imprevisibilidad de quienes tienen el poder también puede dificultar medir con precisión el valor de bienes y servicios. Sientes confusión e incomodidad al adaptarte a un mundo donde el valor del dinero ya no está vinculado a una mercancía física como el oro.

La Historia del Dinero

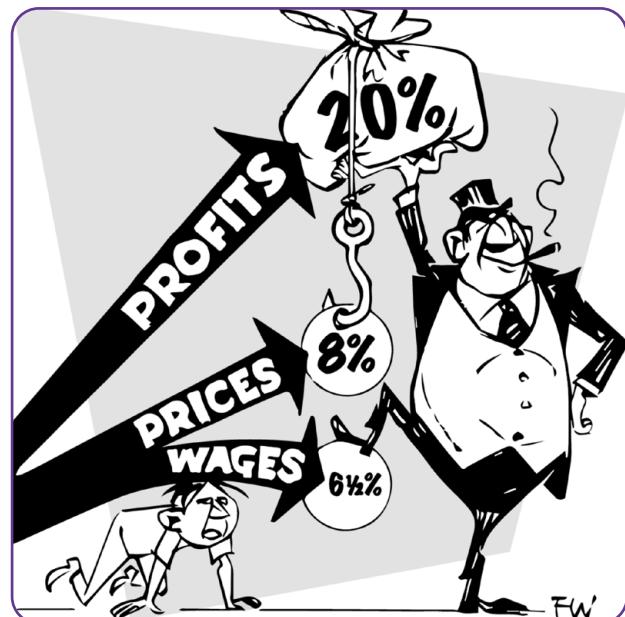
Observas los impactos de este cambio en la economía global y comienzas a cuestionar la estabilidad y confiabilidad de las monedas fiduciarias. Te das cuenta de que en este mundo moderno, el dólar ya no es fijo y consistente como lo era cuando estaba vinculado al oro, sino que se vuelve sujeto a fluctuaciones. Esto dificulta el uso del dólar como unidad de cuenta, ya que su valor se ve afectado por diversos factores, como la inflación (aumento de precios), tasas de interés, la fuerza de la economía del país, eventos políticos, especulación del mercado y la demanda en el comercio internacional. Puede ser un momento confuso e impredecible mientras intentas navegar por el valor constantemente cambiante del dólar y su impacto en tu vida diaria.

A pesar de los esfuerzos por mejorar la calidad de vida a través de sistemas monetarios modernos, mayor eficiencia, mayor acceso a la información y comunicación mejorada, la mayoría de las personas ven disminuir sus niveles de vida debido a:

- ☀ Abuso de la centralización.
- ☀ Aumento de precios.
- ☀ Estancamiento de los salarios reales.
- ☀ Debilitamiento de las monedas.
- ☀ La necesidad de gastar más dinero por menos cosas.

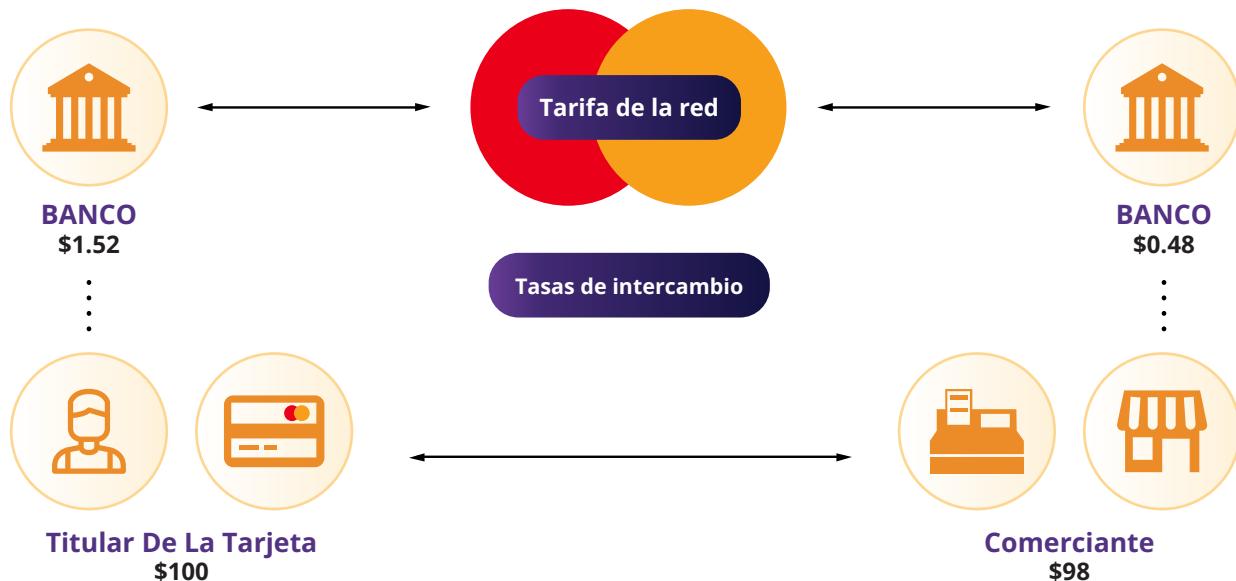
Esto presenta desafíos para aquellos con recursos económicos más bajos, que pueden tener acceso limitado a educación, crédito, recursos, redes sociales y representación política, lo que podría llevar a desventajas en su capacidad para tener éxito.

Como resultado, parece que los ricos siguen enriqueciéndose y los pobres siguen empobreciéndose.



3.1.4 De Papel a Plástico

Hoy en día, hemos recorrido un largo camino desde la introducción de la primera tarjeta de crédito en la década de 1950. Con un simple deslizamiento de plástico, podemos comprar lo que queramos, cuando queramos, sin ningún problema. Es como abrir un mundo de posibilidades infinitas, y la emoción de descubrir lo que contiene es palpable... o eso pensábamos. Poco sabíamos que nuestra dependencia del crédito tendría efectos secundarios dolorosos, como aumentar el costo total de los bienes e incentivar una cierta economía condenada al fracaso.



A medida que avanza la tecnología, también lo hace la forma en que manejamos el dinero. Internet se convierte en un jugador importante en el mundo financiero, con la banca en línea y sitios web de comercio electrónico que hacen posible gestionar y gastar dinero completamente en línea.

El surgimiento del dinero digital marca el siguiente salto significativo en esta evolución, ofreciendo nuevas posibilidades y remodelando la forma en que realizamos transacciones financieras.

3.2 Moneda Digital

Ahora, sumérjamonos en el emocionante mundo del dinero digital. Las monedas digitales, a diferencia de las tradicionales, existen únicamente en forma electrónica. Se almacenan y se intercambian mediante computadoras y software especializado.

La moneda digital permite a las personas enviar su dinero a través de Internet. Al igual que el correo electrónico nos permite enviar mensajes instantáneamente y sin costos de envío, las monedas digitales nos permiten enviar y recibir valor instantáneamente y con muy poco costo.

Las monedas que usamos hoy en día se están volviendo cada vez más digitales. Solo una pequeña fracción del suministro de dinero realmente existe en forma de monedas y billetes de papel. Los bancos y los servicios bancarios proporcionan a sus usuarios aplicaciones para intercambiar dinero sin problemas a través de Internet. Pero, ¿de dónde viene el dinero?

En este capítulo, hemos sido testigos de la transformación desde el dinero sonante, representado por el oro, hasta el dinero no sonante en forma de papel y, ahora, moneda fiduciaria digital. En el próximo capítulo, exploraremos cómo funciona el actual sistema monetario fiduciario y cómo llegó a existir.

Capítulo #4

¿Qué es el Dinero Fiat y Quién lo Controla?

4.0 Introducción

4.1 Breve historia del dinero fiat

4.2 El Sistema Fiat

4.2.1 Un sistema monetario por decreto

4.2.2 Banca de Reserva Fraccional: un sistema alimentado por deuda

Actividad: Banca de Reserva Fraccional

4.2.3 ¿Quién controla el sistema fiat y cómo se benefician?

4.3 Monedas Digitales de Banco Central: El Futuro del Dinero Fiat

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

¿Qué es el Dinero Fiat y Quién lo Controla?

4.0 Introducción

La historia de la humanidad es la historia de la pérdida de valor del dinero.

Milton Friedman

Vimos en el capítulo anterior cómo evolucionó el dinero a lo largo del tiempo y cómo nuestro sistema monetario pasó de ser sólido a ser un dinero no respaldado, dando forma al mundo en el que vivimos hoy. Este capítulo profundiza en cómo estos desarrollos llevaron al sistema fiat actual y cómo funciona ese sistema fiat.

Entonces, ¿cómo se ve este sistema Fiat y cómo llegó a existir?

Para responder a esta pregunta, debemos comenzar centrándonos en el dólar estadounidense, la moneda de reserva actual del mundo, que desempeña un papel dominante en el mundo actual. Cada país, directa o indirectamente, siente el impacto de las decisiones tomadas con respecto al dólar estadounidense. Para comprender verdaderamente cómo opera el sistema fiat en su país, es esencial desentrañar los hilos históricos que lo conectan con el lugar de nacimiento del sistema fiat: los Estados Unidos de América.

4.1 Breve historia del dinero fiat

1815-1933	1913	1933	1934	1944	1971	1980
Estándar de oro	Creación del Banco Central (USA) llamado "la Reserva Federal"	Orden Ejecutiva 6102. Todo ciudadano estaba obligado a entregar su oro a un tipo de cambio de \$20,67 la onza.	Ley de Reserva de Oro. Robar riqueza al pueblo devaluando el dólar en un 40% a \$35 por onza de oro.	Acuerdo de Bretton Woods: el dólar estadounidense se convirtió en la moneda de reserva mundial dominante	Nixon Shock, que dio origen al sistema fiduciario al poner fin a la canjeabilidad de dólares estadounidenses por oro.	El valor del oro aumentó de \$35 por onza en 1970 a \$870 por onza en 1980, lo que provocó una pérdida de valor del dinero de la gente en un 96% en sólo 10 años

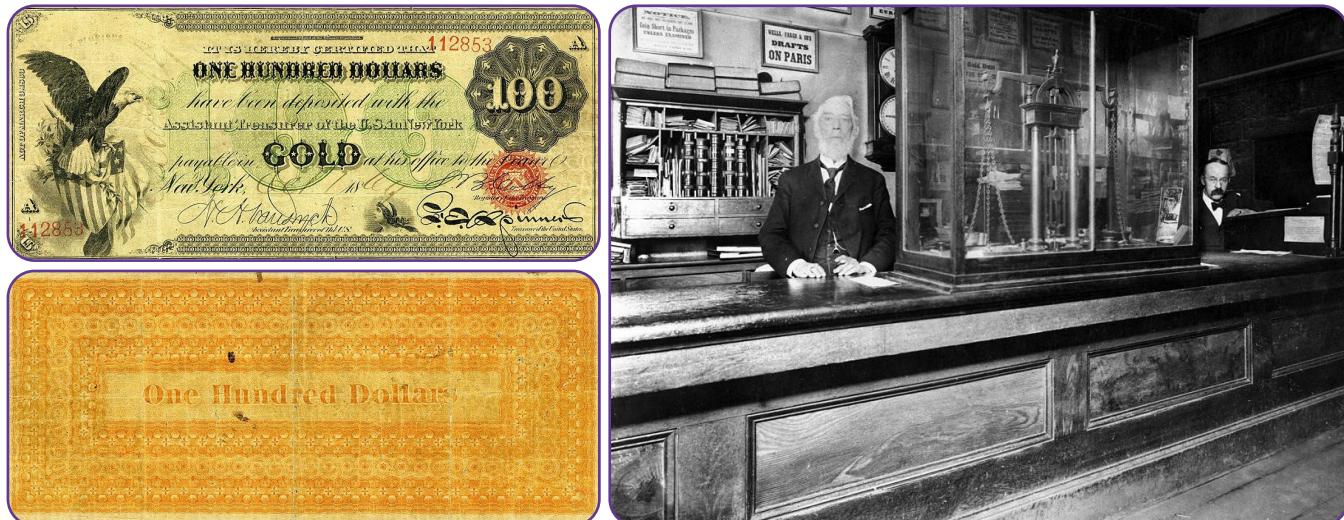
Línea de tiempo

El siglo XIX fue una época en la que las civilizaciones de todo el mundo descansaban en un estándar de dinero sólido utilizando metales preciosos como dinero, porque eran escasos, duraderos y reconocibles. A medida que creció el comercio global, transportar grandes cantidades de metal se volvió un reto desafiante, lo que llevó a la aparición de almacenes de oro y plata. Estos almacenes almacenaban de manera segura los metales valiosos de las personas y proporcionaban certificados en papel canjeables por cantidades específicas de oro o plata.



Capítulo #4

A cambio de depositar su dinero, los individuos recibían certificados en papel directamente vinculados a la cantidad exacta de oro o plata que almacenaban. Este vínculo directo entre los certificados en papel y el dinero tangible de mercancía marcó los primeros pasos de lo que ahora reconocemos como bancos.



Inicialmente, los bancos tenían como objetivo resguardar el dinero de los clientes, pero más tarde se involucraron en prácticas de préstamo arriesgadas, emitiendo certificados por oro que no poseían. Esta práctica representaba la amenaza de corridas bancarias si demasiados clientes reclamaban su dinero simultáneamente.



Para abordar el riesgo, los bancos colaboraron con los gobiernos para establecer un sistema que legalizara la re-lending. En 1913, crearon la Reserva Federal, un banco central responsable de generar nuevos certificados en papel y rescatar a los bancos en problemas. A nivel mundial, los gobiernos reconocieron el valor del oro y la plata, lo que llevó a conflictos y guerras por el control. En los años previos a la Segunda Guerra Mundial, líderes como Lenin, Stalin, Churchill, Roosevelt, Mussolini y Hitler se apoderaron

A principios de la década de 1930, ocurrió un cambio significativo en la forma en que el dinero estaba respaldado por activos en los Estados Unidos. En ese momento, las personas solían tener una gran parte de su riqueza en forma de oro. Sin embargo, en 1933, el Presidente Roosevelt emitió la Orden Ejecutiva 6102, que exigía que cada ciudadano entregara su oro. Esto no fue un intercambio voluntario: se requería que las personas entregaran su oro, y si se negaban, enfrentaban severas sanciones.

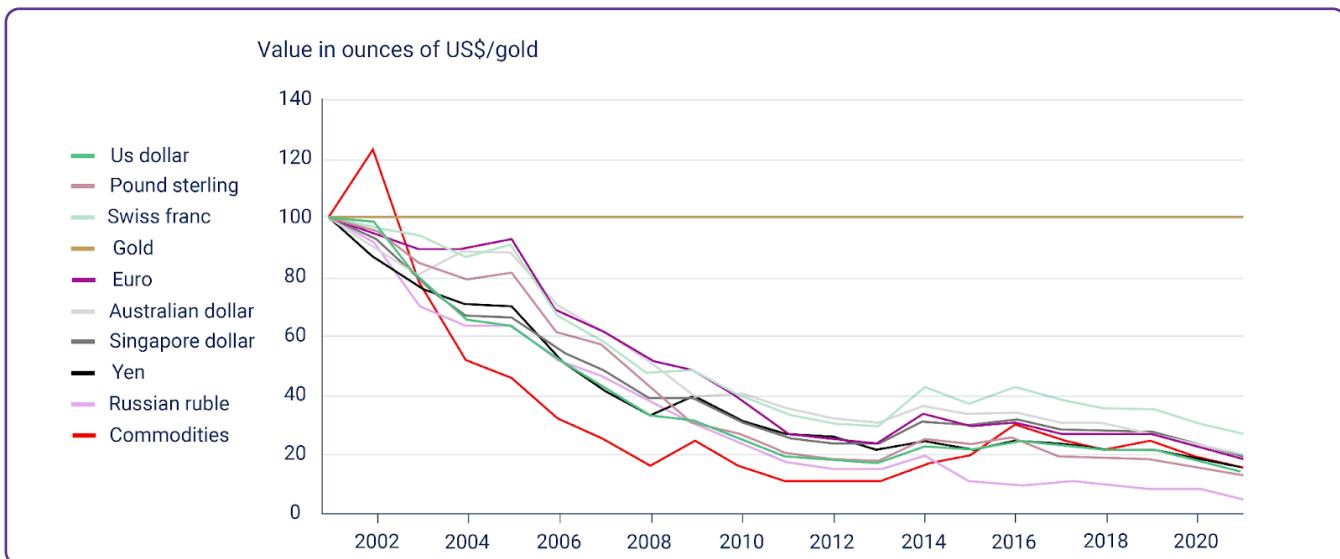
El gobierno fijó la tasa de cambio en \$20.67 por onza de oro. Esto significaba que por cada onza de oro que una persona tuviera, recibían certificados en papel equivalentes a \$20.67. Las personas tenían que aceptar estos dólares en papel, con la esperanza de que algún día pudieran volver a cambiarlos por oro.



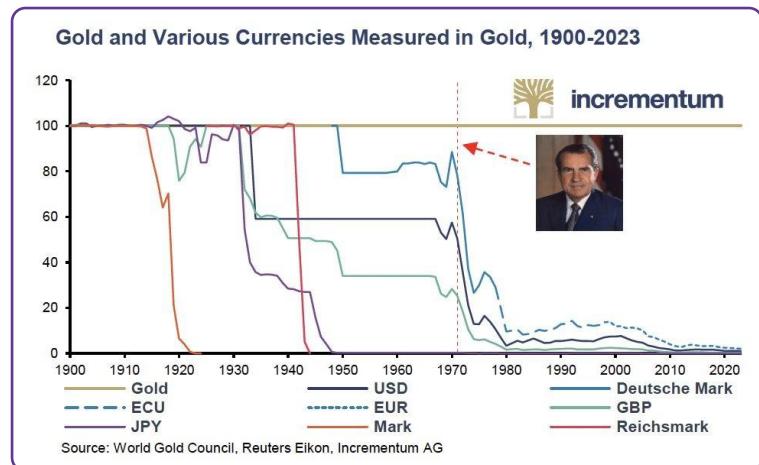
¿Qué es el Dinero Fiat y Quién lo Controla?

En 1934, la subsiguiente Ley de Reserva de Oro hizo posible intercambiar los dólares de papel de las personas por oro nuevamente. Pero esta vez hubo un truco, el gobierno deliberadamente devaluó los dólares de papel al aumentar el tipo de cambio a \$35 por onza de oro. Esta devaluación afectó mucho más a las personas trabajadoras de las clases media y baja, ya que significó que sus ahorros, que antes valían más, ahora valían menos debido a la disminución del valor del papel dólar.

Después de la Segunda Guerra Mundial, el acuerdo de Bretton Woods en 1944 estableció el dólar estadounidense como la moneda de reserva mundial, y podía ser intercambiado por oro. Sin embargo, este vínculo entre el dólar estadounidense y el oro se rompió en 1971 cuando el Presidente Nixon puso fin a la convertibilidad del dólar estadounidense en oro. Esto marcó un cambio significativo, que llevó a la adopción de un sistema de dinero fiduciario en el que el valor de la moneda no está respaldado por una mercancía física como el oro, sino por la confianza y la credibilidad de las personas que lo utilizan. A medida que los gobiernos y los bancos centrales retuvieron la mayor parte del oro de la gente, el valor del oro se disparó, alcanzando los \$870 por onza en 1980.



En conclusión, la historia de cómo la sociedad humana pasó de un patrón monetario sólido a un patrón monetario no sólido (fiduciario) es la historia de cómo los gobiernos y los bancos capturaron los metales preciosos de sus ciudadanos. Mientras que el dinero real acabó en los bolsillos de los gobiernos y los bancos, la gente se quedó con trozos de papel cuyo único valor proviene de que los gobiernos exigen su uso.



4.2 El Sistema Fiat



El problema fundamental con la moneda convencional es toda la confianza que se necesita para que funcione. Se debe confiar en que el banco central no devalúe la moneda, pero la historia de las monedas fiat está llena de violaciones de esa confianza

Satoshi Nakamoto



La humanidad hizo la transición de un dinero sólido controlado por muchos, a un dinero no sólido controlado por pocos. Entonces, ¿cómo funciona exactamente este sistema?

4.2.1 Un sistema monetario por decreto

El sistema fiat se caracteriza por su carácter obligatorio, impuesto a las personas a través de leyes de curso legal. El término "Fiat", que proviene del latín, significa "por decreto", representando una directiva emitida por las autoridades.

A diferencia del dinero respaldado por activos tangibles, como el oro, el dinero fiat carece de tal respaldo. En su lugar, su uso está mandatado por la ley. Monedas cotidianas como el dólar, el euro, la libra, el yuan, el peso y otras caen bajo la categoría de dinero fiat.

Ley de curso legal: Una ley que obliga a todos los ciudadanos a aceptar un tipo específico de moneda.



El valor del dinero fiat se basa en la creencia de que puede ser intercambiado por bienes y servicios y la ilusión de que mantendrá su valor con el tiempo. El dinero fiat es comparable a una entrada de concierto; su valor no reside en el papel de la entrada en sí, sino en la seguridad de que la banda (el gobierno y su banco central) ofrecerá un gran espectáculo (proporcionar estabilidad económica).

Ventajas del dinero fiat

- 💡 **Facilidad de uso:** El dinero fiat es conveniente para transacciones cotidianas.
- 💡 **Menores costos y riesgos:** El dinero fiat no requiere de una seguridad pesada como el oro, lo que lo hace más barato y seguro.

Consecuencias del Dinero Fiat

- 💡 **Riesgos de inflación:** Los precios pueden subir continuamente, causando inflación e instancias históricas de hiperinflación.
- 💡 **Control centralizado y manipulación:** Grupos pequeños pueden influir y manipular el sistema, llevando a la censura y confiscación.
- 💡 **Riesgo de contraparte:** Si el gobierno enfrenta desafíos, la moneda puede perder valor.
- 💡 **Potencial para el abuso:** El sistema puede ser mal utilizado, resultando en corrupción y pérdida de confianza.

¿Qué es el Dinero Fiat y Quién lo Controla?

Mercancía vs Fiat: Imagina la Diferencia

Recuerda: antes de que surgiera la moneda fiat, los gobiernos acuñaban monedas a partir de una materia prima valiosa, escasa y difícil de obtener, como el oro o la plata, o imprimían dinero en papel que podía ser canjeado por una cantidad fija de una materia prima física. Esto era el sistema respaldado por mercancías.

Ahora, en el sistema fiat, es más parecido a tener dinero de Monopoly. El dinero en el sistema fiat consiste en pedazos de papel impresos por el banco central, y las políticas del gobierno influyen directamente en su valor. El gobierno y los bancos centrales son básicamente los "banqueros del juego de Monopoly" que controlan cómo funciona el juego, quién recibe qué y cuánto vale. En otras palabras, el gobierno promete hacer un buen trabajo en la gestión del sistema monetario.

En conclusión, las monedas fiat solo tienen valor porque el gobierno obliga a su uso; no hay utilidad en sí misma para el dinero fiat.

En resumen, el sistema fiat es un juego de confianza donde el valor de nuestro dinero depende de las promesas de quienes están a cargo, y la gente solo puede esperar que su gobierno actúe en beneficio de todos. A continuación, veremos cómo los bancos crean nuevo dinero, quiénes están involucrados y cómo afecta a la economía.

4.2.2 Banca de Reserva Fraccionaria: un sistema alimentado por deuda

Es bastante conveniente que la gente de la nación no entienda nuestro sistema bancario y monetario, porque si lo hicieran, creo que habría una revolución antes de mañana.

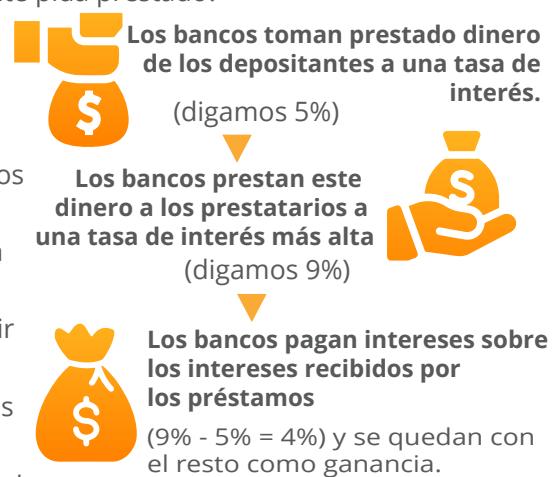
Henry Ford

La banca de reserva fraccionaria es una de las partes principales del sistema fiat. Permite a los bancos prestar la mayoría de los depósitos de sus clientes a otros clientes. ¿Alguna vez te has preguntado por qué los bancos ofrecen tantos servicios a sus clientes? Aunque pueda parecer que son generosos, es importante recordar que los bancos son negocios y su objetivo principal es obtener beneficios. Pero, ¿cómo obtienen beneficios si están prestando dinero dejando que la gente pida prestado?

Además de ganar intereses sobre los depósitos, los bancos generan ingresos de otras maneras, incluyendo:

- ✿ Cobrar intereses sobre los préstamos que otorgan.
- ✿ Cobrar tarifas por servicios como el uso de cajeros automáticos y el mantenimiento de cuentas.
- ✿ Ganar dinero a través de inversiones, como la compra y venta de valores o la inversión en bienes raíces.
- ✿ Mantener un porcentaje de los préstamos en reserva e invertir o prestar el resto.
- ✿ Pagar intereses sobre los depósitos y cobrar tarifas en cuentas corrientes y de ahorro.

Cuando un banco recibe un depósito, está obligado a mantener solo una fracción (requisito de reserva) y puede prestar el resto.





Capítulo #4

Por ejemplo, si depositas \$100 con un requisito de reserva del 10%, el banco puede prestar \$90, manteniendo solo \$10 como reservas. El prestatario deposita \$90 en otro banco, permitiendo que el ciclo continúe. A pesar del depósito inicial de \$100, el dinero total en la economía crece a \$271, aparentemente apareciendo de la nada, un fenómeno conocido como el efecto multiplicador.

Este proceso lleva a un sistema monetario impulsado por la deuda ya que los bancos crean nueva moneda con cada préstamo, aumentando la oferta monetaria general. A medida que continúa la banca de reserva fraccionaria, la deuda total en la economía aumenta, contribuyendo a la inflación.

El sistema depende de un ciclo continuo de creación de moneda a través de préstamos, similar a un suministro constante de drogas para un adicto. Sin embargo, si los bancos prestan más dinero del que tienen en reservas y los depositantes corren a retirar dinero simultáneamente, los bancos podrían enfrentar la quiebra.

Aquí, el banco central interviene como prestamista de último recurso, proporcionando nueva moneda para evitar la quiebra de los bancos. El banco central logra esto recomprando activos o inyectando moneda directamente en las cuentas de los bancos. En esencia, los bancos son salvados de la quiebra mediante la inyección constante de nueva moneda por parte de los bancos centrales. Este sistema impulsado por la deuda sistemáticamente rescatado por el banco central resulta en ciclos de auge y crisis.

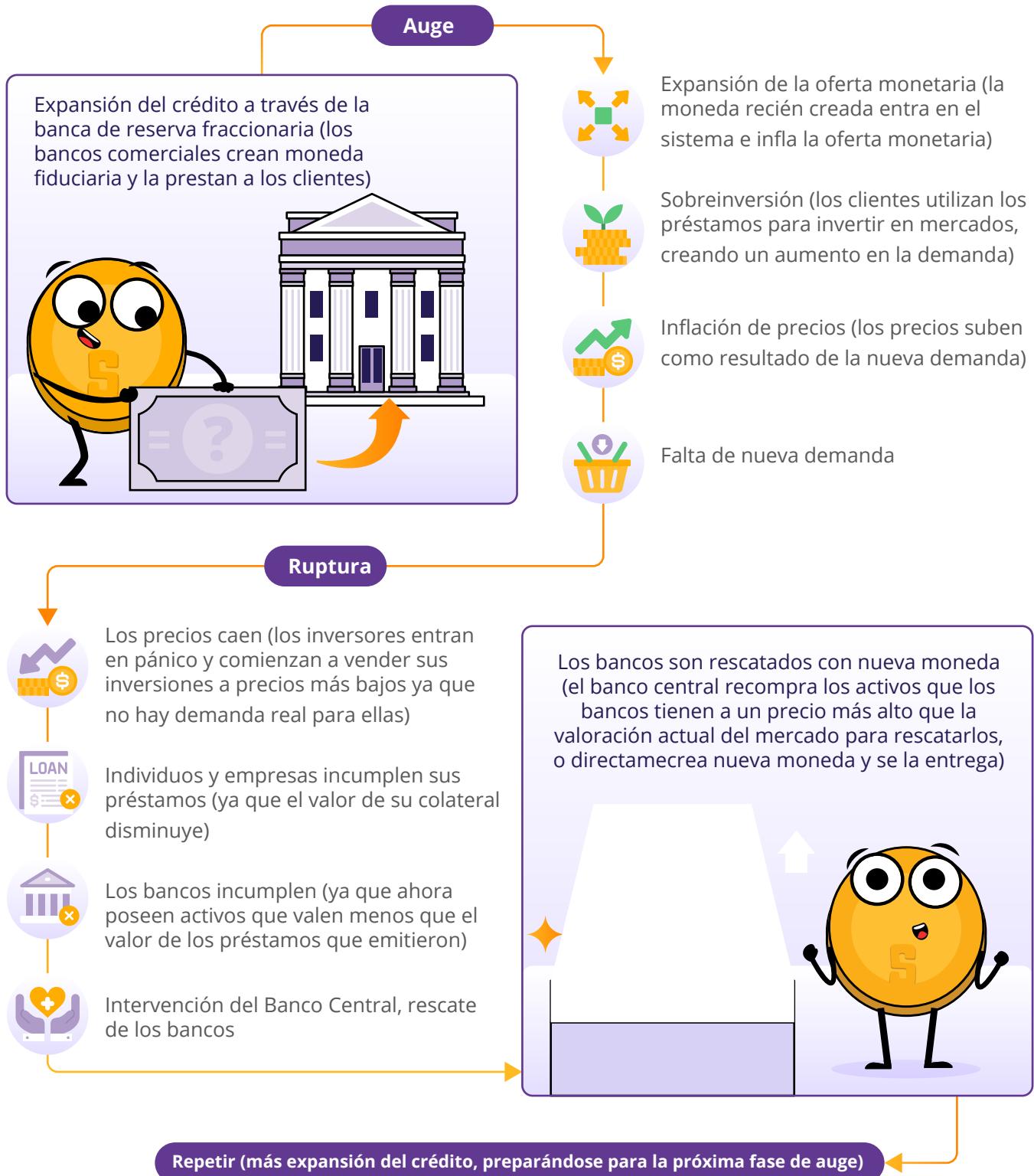
Imagina que tienes un amigo que resulta ser banquero; vamos a llamarlo Dax.

A Dax le encantan las bicicletas, y quiere pedir prestada tu bicicleta porque tiene muchos lugares a donde ir. Le prestas tu bicicleta, y para sorpresa tuya, Dax comienza a prometer la misma bicicleta a muchos otros amigos al mismo tiempo. Con tu única bicicleta real que le prestaste, Dax logra crear más bicicletas imaginarias y comienza a prestarlas a amigos. Cada uno de sus amigos piensa que puede disfrutar de un buen paseo cuando quiera. Pero aquí está la vuelta de tuerca: ¡solo hay una bicicleta real! ¡Todas las demás son imaginarias y solo promesas!

Entonces, ¿qué pasa...? A medida que circulan más bicicletas imaginarias, todos están muy felices, al menos inicialmente. Porque al principio nadie usa la bicicleta al mismo tiempo. Parece que no hay problema. Se siente como si hubiera una abundancia de bicicletas para todos. Así que todos los amigos comienzan a hacer más planes, pensando en todos los lugares a los que irán con sus bicicletas. Sin embargo, aquí es donde la magia comienza a perder su encanto. Un día soleado, todos deciden que es un día perfecto para andar en bicicleta. Todos llegan a la puerta de Dax, emocionados por sacar sus bicicletas imaginarias a dar un paseo. Pero, la realidad golpea: solo hay una bicicleta real. La decepción sigue, y de repente, el valor de los paseos prometidos disminuye.

En el mundo del préstamo con reserva fraccionaria, es una historia similar. Los bancos prestan más dinero del que realmente tienen, y por un tiempo, todos disfrutan de los beneficios. Más dinero circula, y parece que hay suficiente para todos. Pero, si demasiadas personas intentan retirar su dinero al mismo tiempo, el verdadero valor se hace evidente: no hay suficiente para cumplir todas las promesas. Este escenario afecta al bien común y al valor de todos los involucrados. La promesa de abundancia se convierte en un fraude. Así como las bicicletas imaginarias pierden su valor percibido cuando todos quieren un paseo real, el valor del dinero en la economía puede disminuir cuando todos corren a reclamar su parte real. Cuando eso sucede, las personas descubren que el dinero que tienen en un banco no está realmente allí, lo que conduce al pánico, las corridas bancarias e incluso al colapso de economías enteras. Los que están pagando por estos colapsos han sido siempre el mismo grupo: la clase baja y media del mundo.

¿Qué es el Dinero Fiat y Quién lo Controla?



Actividad: Banca de Reserva Fraccionaria

En el siguiente ejercicio, exploraremos cómo la banca de reserva fraccionaria puede conducir a la devaluación de la moneda, la inflación y una disminución del poder adquisitivo. Utilizaremos un ejemplo simplificado que involucra a seis participantes, uno de los cuales actuará como banco, y una tasa de reserva que todavía se utiliza mucho hoy en día: el 10%

- ◆ A acaba de ganar \$100,000 en la lotería y los deposita en el banco (B). Con una tasa de reserva del 10%, B debe mantener \$10,000 en su bóveda y puede prestar los \$90,000 restantes.
- ◆ C solicita el monto máximo (\$90,000) a B y lo utiliza para comprar una casa a D.
- ◆ D deposita los \$90,000 recibidos de C en el banco (B). Los depósitos totales en el banco son ahora de \$190,000.
- ◆ E solicita un préstamo a B, y el banco presta el 90% del nuevo depósito, que son \$81,000.
- ◆ E utiliza el préstamo de \$81,000 para comprar una obra de arte a F, quien luego deposita el dinero en el banco (B). Los depósitos totales registrados son ahora de \$271,000.

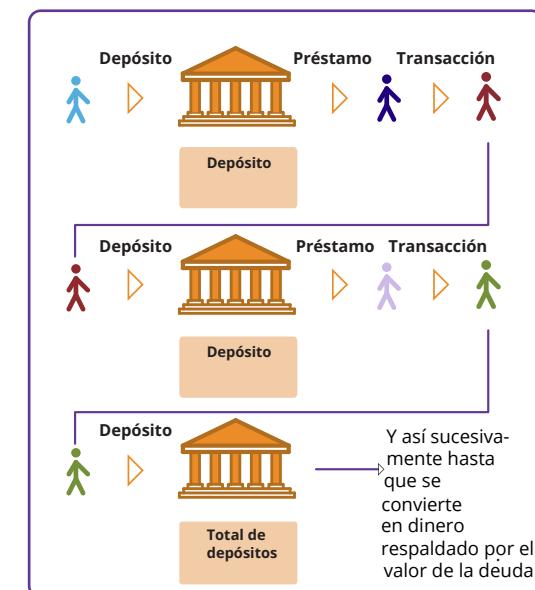
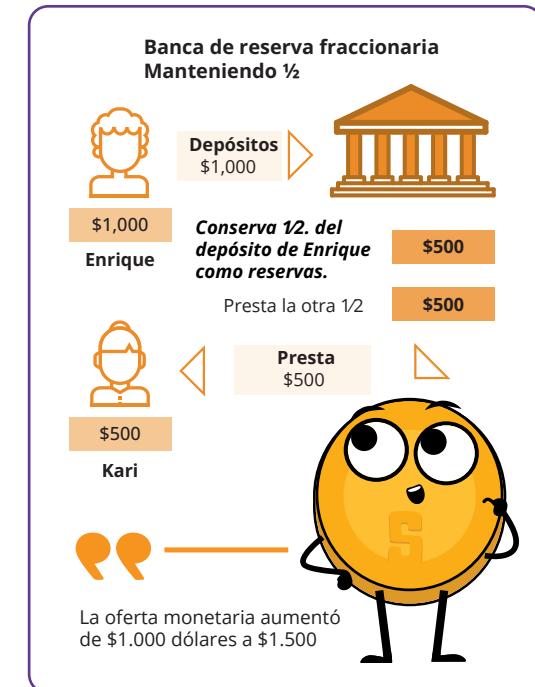
En este escenario, el depósito inicial de \$100,000 ha dado como resultado un total de \$271,000 en depósitos después de circular por la economía.

Si la tasa de reserva se redujera al 1%, la cantidad de dinero creado sería significativamente mayor ($\$100,000 / 0.01 = \$10,000,000$). En este caso, ¿cuánto dinero se crearía realmente con esos \$100,000 si el dinero continúa circulando por la economía?

Es importante tener en cuenta que a partir de 2020, la Reserva Federal (el Banco Central de los Estados Unidos) redujo las tasas de requisitos de reserva al 0% para estimular la economía.

Necesitamos los siguientes voluntarios:

- A** = Depositante (Ganador de la Lotería) (Azul Claro)
- B** = Cajero del Banco (Banco)
- C** = Deudor #1 (Azul Oscuro)
- D** = Dueño de la Propiedad/Depositante (Rojo)
- E** = Deudor n.º 2 (púrpura claro)
- F** = Propietario/Depositante de la galería de arte (verde)



¿Qué es el Dinero Fiat y Quién lo Controla?

4.2.3 ¿Quién controla el sistema fiat y cómo se benefician?

Hay cuatro actores principales: el gobierno, los individuos ricos, el sector financiero y el banco central. Juntos, controlan el sistema fiat.

El Gobierno: El gobierno es como el director del espectáculo fiat. Además de la recaudación de impuestos, se financia mediante nueva deuda (bonos) emitida por el Tesoro. Cuando no hay suficiente demanda de estos bonos, cualquier deuda restante es adquirida por el banco central. Esto significa que pueden seguir realizando sus actividades y persiguiendo sus intereses sin necesidad de aprobación del pueblo. Es como obtener una tarjeta de crédito sin preocuparse por pagar de inmediato. Puede parecer bueno para el gobierno, pero tiene un costo para todos los demás.

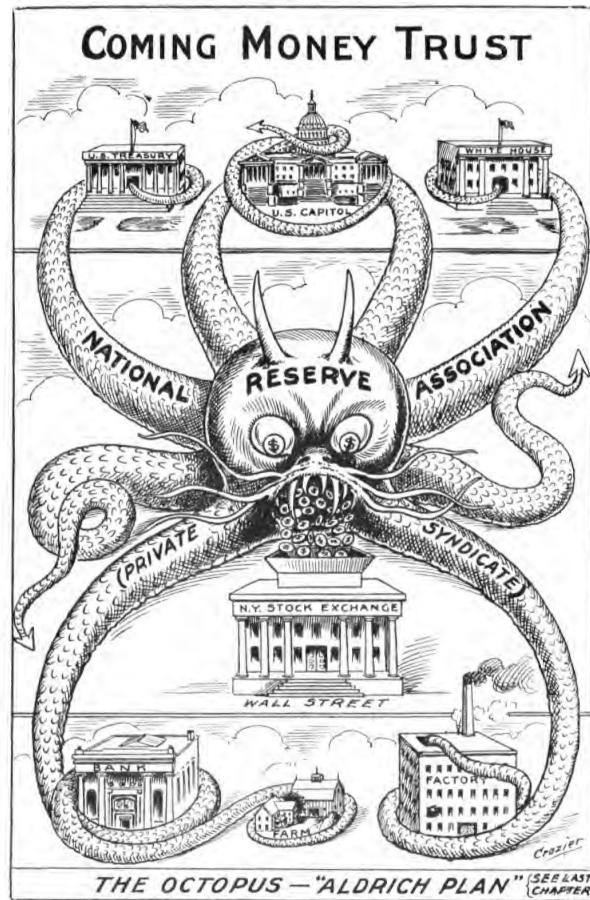
Individuos Adinerados: Los individuos adinerados se benefician mucho del sistema fiat. Con la capacidad de acumular más deudas, pueden invertir en activos como materias primas, bienes raíces y acciones, creando nueva riqueza casi sin esfuerzo.

Sector Financiero (bancos): Los bancos y otras instituciones financieras no controlan directamente el sistema fiat, pero se benefician enormemente de él. Liberados de responsabilidades, pueden perseguir y acelerar la creación de nueva moneda mediante préstamos con reserva fraccionaria, beneficiándose de mayores ingresos. Los bancos prácticamente no tienen consecuencias, ya que son rescatados con nueva moneda fiat para evitar que todo el sistema colapse.

El Banco Central: El banco central es quien tira de los hilos, supuestamente controlando el crecimiento de la oferta monetaria. Pero aquí está el truco: el banco central también está sujeto a las leyes del gobierno, sirviendo a los intereses del gobierno. Es como un titiritero controlado por otro titiritero. El banco central puede parecer el que está a cargo, pero está sirviendo indirectamente los deseos del gobierno de imprimir dinero de la nada cuando lo necesita.

Cómo se benefician: Estos grupos se benefician de diversas maneras, creando una red compleja de control. El gobierno obtiene fondos sin consecuencias inmediatas, los individuos adinerados y los bancos ganan dinero sin esfuerzo, y el banco central mantiene el espectáculo en marcha. Mientras tanto, el resto de la población puede sentir los efectos, enfrentando desafíos a medida que se desarrolla el sistema.

Al final, los titiriteros del sistema fiat crean un espectáculo donde unos pocos se benefician enormemente, pero muchos se preguntan sobre la equidad del escenario financiero en el que se encuentran.



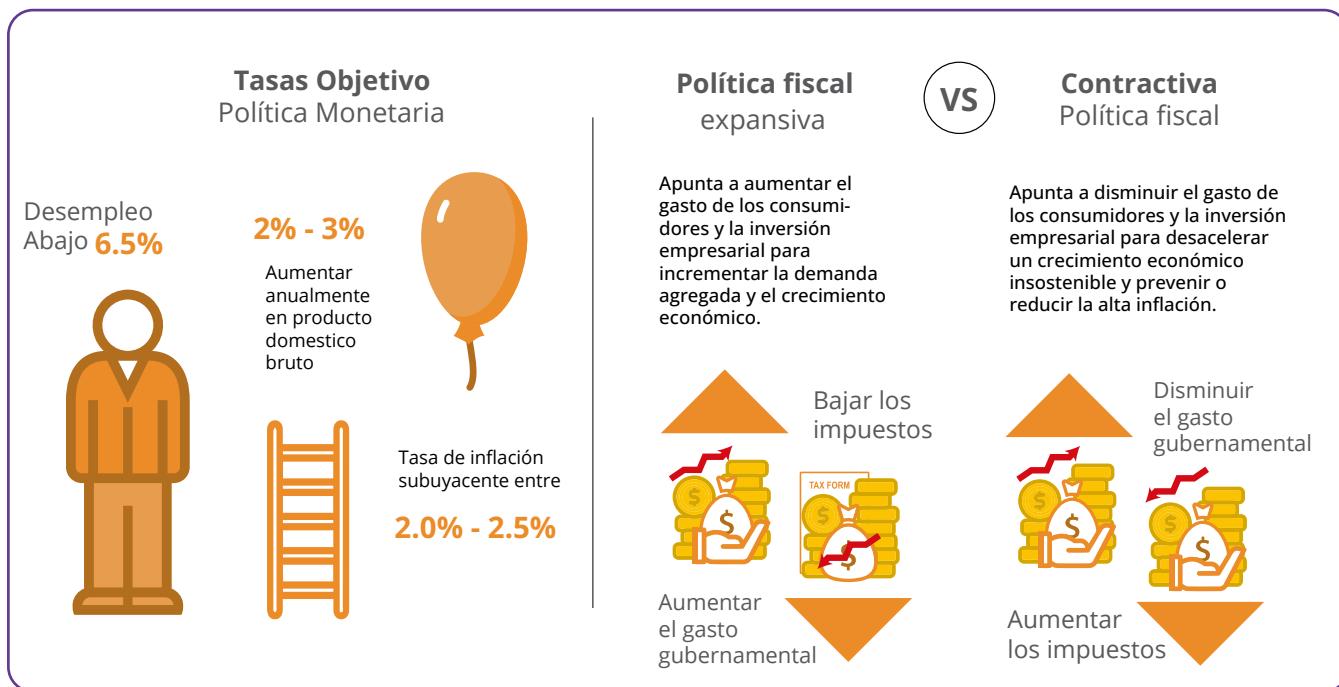
El papel de los bancos centrales

Los bancos centrales moldean silenciosamente cómo funciona una economía. Su trabajo oficial es asegurar la estabilidad, la integridad y "mantener las cosas estables", pero sus métodos revelan un lado más misterioso. Los bancos centrales trabajan en estrecha colaboración con los gobiernos y manejan la política monetaria, controlando la oferta de dinero con herramientas como las tasas de interés. En tiempos de crisis, imprimen dinero de la nada e inyectan en la economía a través de los bancos comerciales, haciendo parecer que todo está bien.

No solo supervisan las cosas; los bancos centrales regulan los bancos comerciales, establecen las reglas del juego e intervienen para ayudar cuando los bancos tienen problemas (actuando como prestamistas de última instancia). Esta red de control, aunque parece protectora, hace que la economía y los bancos dependan aún más de ellos.

Comprender de dónde provienen los billones de dólares en fondos de estímulo, y quién decide su asignación, es fundamental para comprender el sistema financiero en su conjunto. Los gobiernos utilizan varias herramientas para gestionar la oferta de dinero en momentos específicos.

Los bancos centrales y los gobiernos pueden utilizar herramientas de política monetaria y fiscal para influir en la oferta de dinero y en la economía. Por ejemplo, la Reserva Federal de los Estados Unidos (La Fed) utiliza la política monetaria para ajustar las tasas de interés, lo que afecta la cantidad de dinero en circulación. Por otro lado, la política fiscal implica el uso de políticas de gasto e impuestos para influir en la actividad económica.



¿Qué es el Dinero Fiat y Quién lo Controla?

Las políticas de tipo de cambio, los choques de oferta y los controles de precios sirven como herramientas adicionales para regular la oferta de dinero e impactar el comercio y la economía. Si bien estas políticas tienen como objetivo estabilizar los precios y controlar la inflación, la intervención a menudo conduce a ciclos de auge y caída, creando desafíos para todos los que utilizan la moneda controlada.

Ejemplo: "Demasiado grande para fracasar" se refiere a instituciones financieras tan grandes e interconectadas que su fracaso tendría repercusiones catastróficas en todo el sistema financiero. Durante la crisis financiera de 2008, varios grandes bancos fueron considerados "demasiado grandes para fracasar", lo que llevó al gobierno de Estados Unidos a intervenir y proporcionar rescates para evitar su colapso.

Uno de los ejemplos más destacados de una institución "demasiado grande para fracasar" durante la crisis financiera fue el banco de inversiones Lehman Brothers. Cuando Lehman Brothers se declaró en quiebra en septiembre de 2008, desencadenó una serie de eventos en efecto domino, incluida la casi caída del gigante de seguros AIG y una fuerte caída en el mercado de valores. El gobierno de Estados Unidos tuvo que intervenir y proporcionar rescates a otras importantes instituciones financieras para evitar un mayor caos y proteger la economía en general.

Comprender cómo funcionan estas políticas es vital para comprender las limitaciones de los sistemas monetarios fiat centralizados. Hasta que no comprendas el problema, no reconocerás la solución. Ahora que hemos cubierto cómo ha funcionado el sistema fiat en el pasado y en el presente, discutiremos cómo se ve actualmente el futuro del fiat: las Monedas Digitales del Banco Central, o (CBDCs, por sus siglas en inglés).

4.3 Monedas Digitales de Bancos Centrales: El Futuro del Dinero Fiat

Las Monedas Digitales de Bancos Centrales (CBDC, por sus siglas en inglés) son el próximo paso de las monedas fiat. A diferencia de la combinación de billetes físicos, monedas y pagos digitales, las CBDC son formas totalmente digitales de monedas fiat emitidas por gobiernos y controladas por bancos centrales.

Imagina la moneda que usas todos los días, pero sin presencia física, sin monedas para hacer sonar en tu bolsillo ni billetes para doblar y desdoblar. Lo que distingue a las CBDC es el nivel elevado de control y monitoreo que ofrecen a gobiernos y bancos centrales. Con las CBDC, las autoridades obtienen una visibilidad sin precedentes en las transacciones financieras, facilitando el rastreo y la regulación del flujo de dinero.

Gobiernos y bancos centrales pueden ajustar fácilmente la forma y la oferta de las CBDC, manipular tasas de interés y desplegar herramientas de política monetaria y fiscal con mayor precisión. En esencia, las CBDC proporcionan un medio más eficiente para que las autoridades influyan y gestionen su moneda fiat.

Aunque las CBDC parecen ser el futuro del dinero fiat, el sistema monetario actual del mundo ya opera en un estándar fiat puro. Las monedas fiat ya no están vinculadas al oro, lo que resulta en un crecimiento exponencial de la oferta monetaria sin restricciones reales.

Ahora que tienes una mejor comprensión de cómo opera el sistema fiat, es hora de explorar sus consecuencias en el capítulo 5.

Capítulo #5

Cómo Los Problemas Conducen a Soluciones

5.0 Introducción al problema

5.1 Disminución del Poder Adquisitivo

5.1.1 Inflación monetaria y su efecto en el poder adquisitivo

Actividad: Los Efectos de la Inflación — Una Actividad de Subasta

5.2 La Carga Global de Deuda y la Desigualdad Social

5.2.1 Impacto en el individuo — Pérdida de Poder Adquisitivo

5.2.2 Impacto en la sociedad — Aumento de la Desigualdad de Riqueza

Actividad - Consecuencias del Sistema Fiat

5.2.3 La Carga Global de Deuda

5.3 Los Cypherpunks y la búsqueda de una moneda descentralizada

5.3.1 Los Cypherpunks

5.3.2 Sistemas Centralizados vs. Descentralizados

5.3.3 Breve Historia de las Monedas Digitales

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

Cómo Los Problemas Conducen a Soluciones

5.0 Introducción al problema



Quien controla el volumen de dinero en nuestro país es el dueño absoluto de toda la industria y el comercio.. cuando te das cuenta de que todo el sistema es muy fácilmente controlado, de una forma u otra, por unos pocos hombres poderosos en la cima, no necesitarás que te digan cómo se originan los períodos de inflación y depresión

James A. Garfield, Presidente de los Estados Unidos



En el Capítulo 4, aprendiste que el mundo financiero se basa en un sistema que quizás no sea tan sólido como parece. El sistema fiduciario, sostenido por constantes adiciones de dinero en papel, parece beneficiar a unos pocos más que a muchos. Este capítulo revela lo que significa el sistema fiduciario para la gente común y la sociedad. Finalmente, exploramos la historia de un grupo de individuos que notaron los problemas y trabajaron silenciosamente para encontrar una solución que pudiera cambiar el futuro de la sociedad humana.

5.1 Disminución del Poder Adquisitivo

5.1.1 Inflación monetaria y su efecto en el poder adquisitivo

La inflación monetaria es el aumento en la oferta de dinero dentro de una economía, impactando directamente a la persona promedio al reducir su poder adquisitivo. El ciclo de la inflación de precios comienza cuando hay más dinero en circulación. Esto, a su vez, aumenta la demanda de bienes y servicios, lo que finalmente hace que los precios suban.

Imaginemos un pequeño grupo de amigos: Alex, Bob y Charlie, cada uno con un dólar en la mano, y hay una botella de agua disponible para la venta. La situación inicial es simple: tres personas con un total de tres dólares y una botella de agua. Ahora, supongamos que alguien, digamos el gobierno local, decide darle un dólar extra a cada amigo. Ahora, tienen colectivamente seis dólares. Con este dinero recién encontrado, todos sienten ganas de comprar esa única botella de agua.

Como los tres amigos quieren la misma botella, comienzan a hacer ofertas entre ellos. La mayor demanda, impulsada por el dinero adicional, los lleva a ofrecer más que el precio inicial por la botella de agua. Al final, la guerra de ofertas hace que el precio de la botella de agua suba. Esta situación refleja una disminución en su poder adquisitivo. Aunque tienen más dinero, no pueden comprar tantas botellas de agua como antes, mostrando el impacto de la inflación en el valor de su dinero.

En este ejemplo, los amigos experimentaron una disminución en su poder adquisitivo porque estaban usando una forma de dinero influenciada por factores externos, como los dólares adicionales introducidos por el gobierno. La falta de control sobre la oferta de dinero, combinada con una mayor demanda, provocó un aumento de precios, lo que dificultó que los amigos compraran la misma cantidad de bienes con sus dólares adicionales.

Esto ilustra cómo el poder adquisitivo de los amigos se vio afectado por factores fuera de su control, enfatizando la importancia de comprender y cuestionar los sistemas que influyen en el valor de nuestro dinero.

Ahora, veamos cómo esto se desarrolla en la vida real.

Actividad: Los Efectos de la Inflación — Una Actividad de Subasta

Objetivo: Comprender el concepto de inflación y cómo afecta los precios de bienes y servicios en una economía.

Definiciones:

 La Oferta Monetaria: la cantidad total de dinero en circulación dentro de una economía en un momento específico. Esto incluye:

- Moneda física, como monedas y billetes
- Cuentas corrientes
- Cuentas de ahorro
- Cuentas de mercado monetario
- Pequeños depósitos a plazo (como CDs) menores a \$100,000.00

 Subasta: Una venta pública en la que bienes o propiedades se venden al más alto postor.

Ejercicio en clase — Sigue las instrucciones a continuación:

1. Recibirs una cantidad aleatoria de dinero de monopoly del profesor. Esto representa la oferta monetaria en una sociedad.
2. Escribe la oferta monetaria total en el cuadro proporcionado.
3. El profesor subastará una barra de chocolate a los estudiantes, para ganar la barra de chocolate, debers hacer la oferta ms alta usando tu dinero de monopoly. Registra la oferta ganadora junto a la oferta monetaria.
4. El profesor luego agregará una cantidad significativa de dinero de monopoly a la oferta monetaria total. Esto representa un aumento en la oferta monetaria en una economía. Ms tarde, aprenders cómo se aade o se reduce la oferta monetaria en una economía.


Las sociedades a menudo pueden ser impredecibles e injustas, como lo ejemplifica la simulación de un maestro que da al azar una cantidad significativa de dinero sólo a unos pocos estudiantes seleccionados. Esto imita situaciones de la vida real donde puede ocurrir una distribución desigual de recursos y oportunidades, resaltando la aleatoriedad e injusticia inherentes en muchas situaciones.

5. El profesor subastará una segunda barra de chocolate a los estudiantes utilizando el mismo proceso que antes. Registra la oferta ganadora junto a la oferta monetaria en el cuadro.
6. El profesor repetirá la subasta por tercera vez.

Cómo Los Problemas Conducen a Soluciones

Ronda	Oferta Monetaria	Puja Ganadora
1		
2		
3		

Conclusión:

1. ¿Cómo afectó el aumento en la oferta monetaria a las ofertas ganadoras por las barras de chocolate?
2. ¿Cuál es la relación entre el aumento de la oferta monetaria y la inflación?
3. ¿Cómo es relevante la oferta monetaria en el mundo real?
4. Cuando se inyecta nuevo dinero en la economía, ¿qué crees que sucederá con los precios de bienes y servicios? ¿Crees que los cambios en los precios son temporales o permanentes, y por qué? ¿Cómo crees que los cambios de precios afectan a los ciudadanos en una sociedad desde una perspectiva a largo plazo?

5.2 La Carga Global de Deuda y la Desigualdad Social

5.2.1 Impacto individual — pérdida de poder adquisitivo

Jaime es un estudiante universitario que vive en un pequeño apartamento. Trabaja a tiempo parcial en una cafetería para pagar sus gastos de vida y matrícula. Tan pronto como comenzó a vivir independientemente, Jaime se volvió bueno en el manejo de su propio libro contable.



Un **libro contable** es un registro detallado de todas tus transacciones monetarias. Ya sea que estés ganando o gastando dinero, un libro mayor te ayuda a llevar un seguimiento de todo.

A principios de 2023, presupuestó \$10,000 para sus gastos de vida durante todo el año, incluyendo alquiler, comida y otras necesidades. Estas fueron sus transacciones para enero de 2023:

Capítulo #5

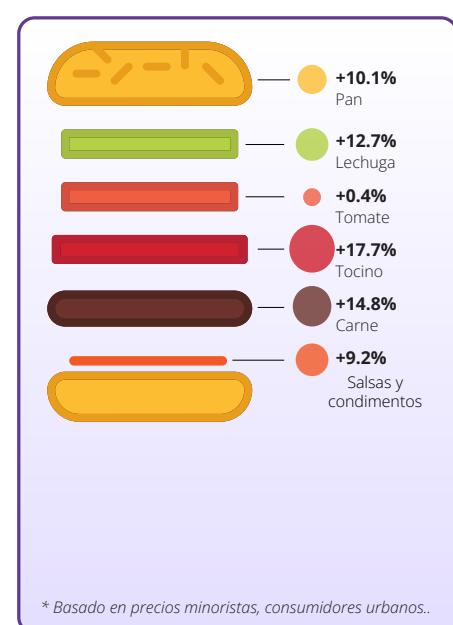
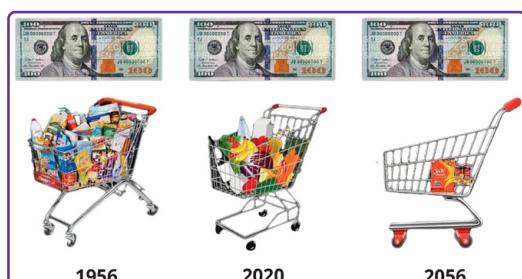
Fecha	Descripción	Cantidad	Tipo	Balance
01/01/2023	Balance Inicial			\$1,600
01/01/2023	Renta de Enero	\$800	Débito	\$800
01/05/2023	Comestibles	\$100	Débito	\$700
01/15/2023	Cheque de pago a tiempo parcial	\$500	Crédito	\$1,200
01/20/2023	Gas para el carro	\$350	Débito	\$850
01/30/2023	Libros de estudio	\$150	Débito	\$700

Este libro contable muestra que el saldo inicial de Jaime fue de \$1,600.00, del cual gastó (un débito) \$800.00 para pagar el alquiler del mes. Luego gastó \$100.00 en comestibles y recibió \$500.00 (un crédito) como pago por su trabajo a tiempo parcial, lo que elevó su saldo a \$1200.00. Luego gastó dinero en gasolina y libros de texto, reduciendo su saldo a \$700.00 al final del mes.

Doce meses después, Jaime almuerza con su abuelo con quien comparte los detalles de su presupuesto para 2024. Jaime nota que su presupuesto no está alcanzando tanto como solía hacerlo, y que su costo de vida ha aumentado significativamente durante el último año. Mientras Jaime se pregunta cómo podría ser esto, su abuelo le muestra la siguiente imagen.

Jaime no puede creer lo que ve. Este es el momento en que descubre que el costo de bienes y servicios aumenta drásticamente con el tiempo, lo que lleva a una disminución en su poder adquisitivo. Su abuelo dice: "En 1956, era solo un joven que comenzaba en el mundo. Recuerdo que solía ganar \$380.00 al mes como trabajador de fábrica. Puede que no parezca mucho, pero era un salario decente en ese momento. De hecho, pude ahorrar lo suficiente para comprar mi propia casa en las afueras".

El abuelo continúa: "Los costos de las cosas eran muy diferentes en el siglo pasado. Por ejemplo, en 2020, comprar 30 barras de chocolate Hershey costaría \$26.14. Sin embargo, si retrocedemos en el tiempo a 1913, el costo de la misma cantidad de barras de chocolate Hershey sería solo \$1.00". Esta diferencia significativa en el precio destaca el cambio en el poder adquisitivo con el tiempo y demuestra cómo el cambio del poder adquisitivo ha cambiado a lo largo de los años debido a la inflación.



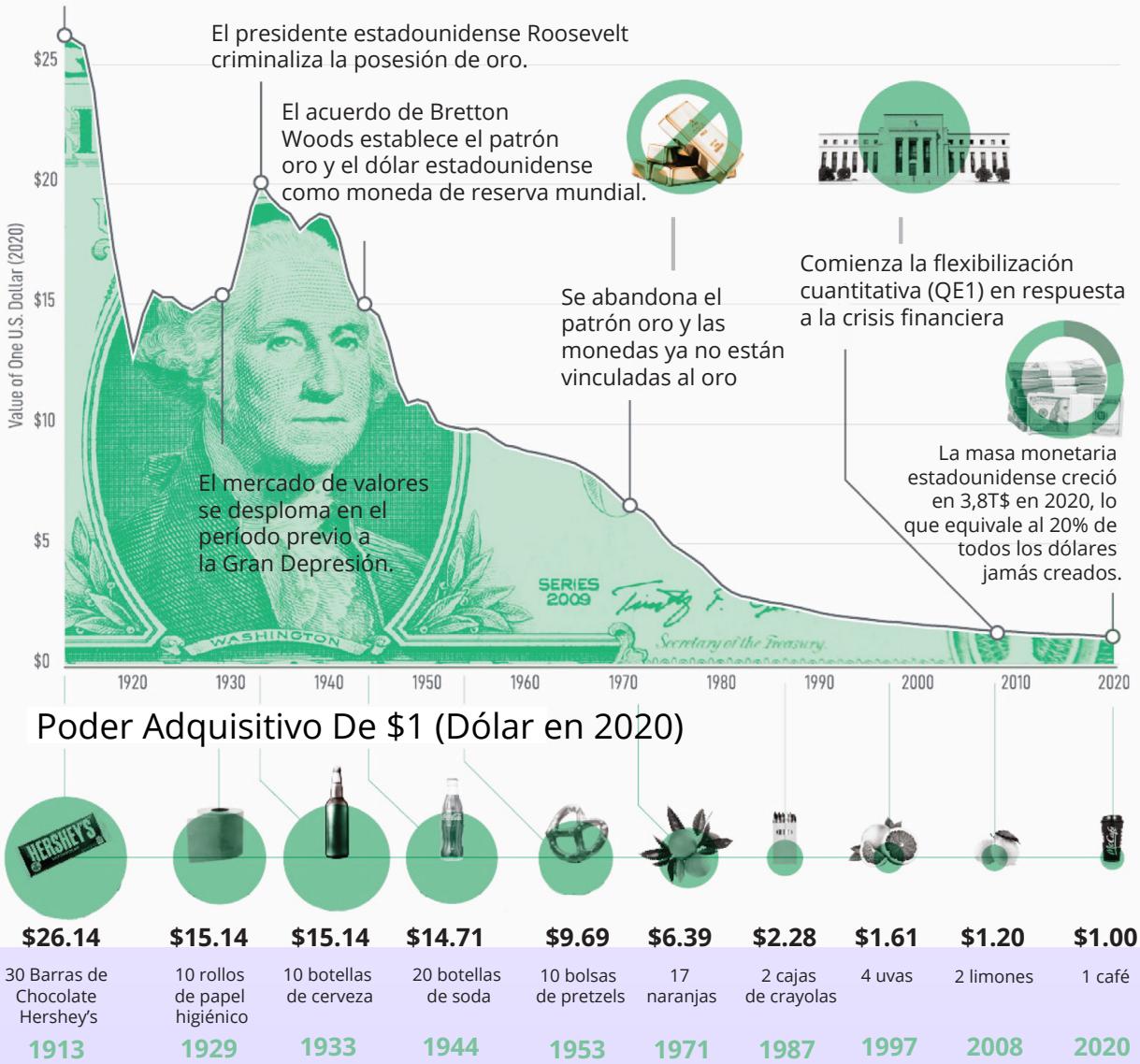
Cómo Los Problemas Conducen a Soluciones

El valor de un dólar

Poder adquisitivo del dólar estadounidense

El poder adquisitivo del dólar estadounidense ha caído drásticamente durante el último siglo debido al aumento de la inflación y la oferta monetaria.

La Ley de la Reserva Federal crea un banco central con la capacidad de gestionar la oferta monetaria del país.



Jaime: "¿Qué? Eso es una locura. No puedo imaginar cuán bajo habría sido mi alquiler en ese entonces en comparación con ahora".

Abuelo: "Bueno, sí, tu alquiler habría sido mucho más barato en ese entonces. Tengo otro ejemplo para ilustrar esto: en ese entonces, \$1.00 te habría comprado aproximadamente 10 bolsas de pretzels. En 2020, pagué \$9.69 por la misma cantidad. Imagina cuánto costarían hoy 10 bolsas de pretzels"

Capítulo #5

Jaime: "Wow, eso es realmente interesante, abuelo. ¿Cómo lo experimentaste tú mismo cuando eras más joven?"

Abuelo: "Oh, Jaime, todo era mucho más barato cuando era joven. Una barra de pan solo costaba \$0.18, y podías comprar un galón de gasolina por solo \$0.29. Es increíble cuánto ha subido el costo de vida".

Después de la conversación con su abuelo, Jaime regresó a casa para echar otro vistazo a su libro mayor. Rápidamente descubrió que necesitaría presupuestar \$1,000.00 adicionales para 2024 para poder comprar la misma canasta de bienes y servicios que adquirió en el año anterior. Esto significa que su poder adquisitivo ha disminuido en \$1,000.00, ya que ahora tiene que gastar más dinero para comprar los mismos bienes y servicios. Mientras que el salario de Jaime solo aumenta ligeramente, sus costos de vida se disparan cada año.

La siguiente tabla muestra los costos de Jaime en el primer año y el segundo año, así como el aumento porcentual en el precio: Para que Jaime pueda seguir sobreviviendo, necesitará trabajar más horas por semana para recibir un adicional de \$1,000.00 y así poder vivir bajo el mismo nivel de vida.

Según la Oficina de Estadísticas Laborales de los Estados Unidos, los precios actuales son 30.39 veces más altos en comparación con los precios de 1913, lo que significa que un dólar hoy solo compra aproximadamente el 3% de lo que compraba un dólar en ese entonces.

Item	Costo Año #1	Costo Año #2	% Aumento
Renta	\$4,000	\$4,500	12.5%
Comestibles	\$2,000	\$2,300	15%
Necesidades	\$4,000	\$4,200	5%
Total	\$10,000	\$11,000	10%

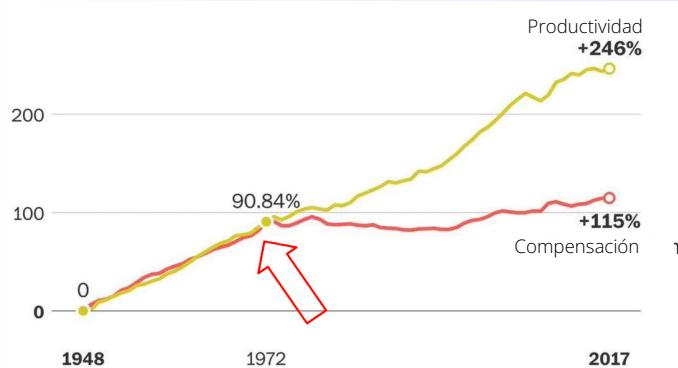
Ahora, imagina que alguien le ofrece a Jaime la opción de viajar en el tiempo: o bien tomar \$100.00 en 1913 o esperar hasta 2023 y recibir apenas \$3.00. Es como decidir entre una racha de compras en el pasado o simplemente obtener un par de pequeños caprichos hoy. La diferencia es enorme, y este ejemplo destaca cuánto ha disminuido el valor del dinero a lo largo de los años.

1938 COST OF LIVING	
<u>LIVING</u>	
New House	\$3,900.00
Average Income	\$1,731.00 per year
New Car	\$860.00
Average Rent	\$27.00 per month
Tuition to Harvard University	\$420.00 per year
Movie Ticket	25¢ each
Gasoline	10¢ per gallon
United States Postage Stamp	3¢ each
<u>FOOD</u>	
Granulated Sugar	59¢ for 10 pounds
Vitamin D Milk	50¢ per gallon
Ground Coffee	39¢ per pound
Bacon	32¢ per pound
Eggs	18¢ per dozen

Cómo Los Problemas Conducen a Soluciones

Cuando pensamos en números, Jaime gana muchos más dólares en un año que lo que ganaba su abuelo, pero los dólares que poseía el abuelo de Jaime eran mucho más valiosos y podían comprar mucho más en ese entonces.

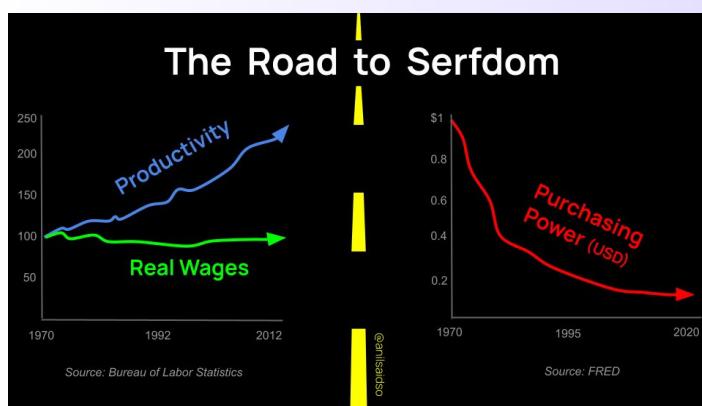
Crecimiento de la productividad y la remuneración por hora (1948 — 2017)



La compensación incluye salarios y beneficios para trabajadores de producción y no supervisores.

En el mundo actual, el significativo impacto de la inflación desalienta a la gente a ahorrar dinero. En cambio, la mayoría opta por gastar su dinero inmediatamente porque su valor disminuye rápidamente. Esta perspectiva pesimista obstaculiza su capacidad de planificar el futuro. Como se ve en el gráfico anterior, el crecimiento salarial del individuo promedio permanece estancado cuando se ajusta a la inflación, lo que significa que no reciben aumentos al mismo ritmo que el valor decreciente de su dinero, a pesar de trabajar más duro.

El ejemplo de Jaime es solo uno de muchos. En el mundo Fiat, es bastante común que los gobiernos creen dinero de la nada para impulsar sus propias agendas y dejar que individuos de todo el mundo enfrenten las consecuencias. Los precios de artículos cotidianos, desde el pan hasta la vivienda, comestibles hasta vacaciones, aumentan cada año. Mientras los ricos se benefician de la inflación al poseer activos, las personas comunes ven cómo su dinero arduamente ganado pierde su valor. ¿El resultado? Individuos y familias en todo el mundo luchan debido a la disminución de su poder adquisitivo.



Personas de todo el mundo se encuentran trabajando en más empleos y más horas sólo para mantener el mismo nivel de vida. Es como estar en una cinta de correr: correr cada vez más rápido pero nunca avanzar. El sistema fiduciario hace que las personas se sientan como si estuvieran en una carrera perpetua contra el aumento de los precios.

En su lucha por mantenerse al ritmo de los crecientes costos, muchos recurren a la deuda, que es como usar una pequeña curita en una herida muy profunda. Las personas toman préstamos o toman decisiones impulsivas solo para salir adelante. El dinero rápido se convierte en una necesidad, y las personas se encuentran en un ciclo donde la supervivencia hoy tiene prioridad sobre la planificación para mañana.

El sistema Fiat, con su constante impresión de dinero, impacta la psicología de la humanidad. Inculca una alta preferencia temporal, centrándose en ganancias a corto plazo en lugar de planificación a largo plazo. Al igual que una solución rápida para un alivio inmediato, las personas en el mundo Fiat tienden a priorizar los beneficios a corto plazo. Es un instinto de supervivencia y crea un ciclo de dependencia, donde las personas buscan cualquier medio para obtener dinero rápido, incluso si no es sostenible o viable a largo plazo.

En esencia, el impacto del sistema Fiat pinta un panorama desafiante para individuos en todo el mundo. En el sistema Fiat, los precios aumentan, los ingresos se estancan y la lucha por sobrevivir se convierte en una batalla diaria. Mientras la clase élite se enriquece, las personas en todo el mundo siguen dependiendo de un sistema que los empobrece cada vez más.

5.2.2 Impacto en la Sociedad — aumento de la desigualdad en la riqueza

En una sociedad basada en dinero sólido, las decisiones financieras del gobierno están vinculadas a la aprobación del pueblo. Sin embargo, en el sistema fiduciario, los gobiernos pueden acumular deudas ilimitadas, a expensas de sus ciudadanos.

El poder de imprimir dinero a voluntad a menudo conduce a la centralización política. El sistema fiduciario permite a los gobiernos acumular deudas masivas, tomando decisiones que benefician a ellos mismos en lugar de a la mayoría. Las superpotencias, como Estados Unidos, obtienen una ventaja competitiva debido a este fenómeno. Pueden imprimir dinero infinitamente para financiar sus planes, incluidas las guerras. Esta capacidad permite a estas naciones dominantes controlar, influir y participar en conflictos geopolíticos, creando un desequilibrio de poder global. Las guerras y las acciones principales para controlar a otros se vuelven financieramente factibles para las superpotencias, mientras que otros sin la misma flexibilidad financiera enfrentan limitaciones.

Bajo el sistema fiduciario, la riqueza no se distribuye de manera equitativa. En cambio, tiende a concentrarse en manos de unos pocos selectos. Este fenómeno es como jugar al Monopoly donde un puñado de jugadores posee casi todos los hoteles y propiedades mientras que la mayoría lucha por mantenerse a flote. El sistema fiduciario se ha convertido en una herramienta para que ciertos grupos concentren la riqueza. La impresión de dinero permite a los gobiernos y su estrecha colaboración con los bancos centrales inyectar más moneda en la economía, y los receptores de este dinero recién creado son aquellos con riqueza y estatus existentes: entidades e individuos poderosos. Estos grupos se benefician del dinero recién impreso antes de que sus efectos negativos, como una disminución en el poder adquisitivo, comiencen a manifestarse a través de la economía.

Cómo Los Problemas Conducen a Soluciones

La desigualdad de riqueza no se trata solo de los que tienen y los que no tienen; se trata de suprimir la movilidad económica. Aquellos de orígenes menos privilegiados encuentran cada vez más difícil escalar la escalera económica, similar a comenzar una carrera con una mochila pesada. La brecha creciente entre ricos y pobres causa problemas para todos, con los ricos dando forma a políticas a su favor. Esto dificulta las cosas para las personas comunes, lo que lleva a la agitación social, una falta de confianza en las instituciones y comunidades que se desmoronan, similar a una casa de naipes. La inestabilidad del sistema fiduciario se manifiesta en incertidumbre económica, agitación política y repercusiones globales cuando el mundo occidental enfrenta una recesión económica.

Este es un fenómeno global, que afecta a las sociedades tanto en naciones desarrolladas como en desarrollo. Los ricos, a menudo operando a escala transnacional, utilizan el sistema financiero global a su favor, ampliando aún más la brecha entre las clases alta y baja.



Bajo el sistema fiduciario, endeudarse se ha convertido en la norma para la humanidad. Gobiernos, instituciones, empresas e individuos en todo el mundo se encuentran inmersos en un mar de deudas. El cambio psicológico hacia considerar la deuda como aceptable tiene sus raíces en el diseño del sistema fiduciario. Durante las últimas décadas, se volvió más fácil para las entidades asumir deudas sustanciales, y para la gente común a menudo se convierte en una necesidad debido al aumento de precios y costos de vida.

El consumismo, un constante impulso de comprar y consumir, lleva a las personas a comprar más de lo que necesitan, lo que resulta en sobreconsumo y desperdicio. Si bien puede parecer una racha de compras interminable, el verdadero costo va más allá de la etiqueta de precio, impactando la psicología y el bienestar de las personas. Se vuelve evidente que el sistema fiduciario no es solo un mecanismo económico. Más bien, es un sistema que moldea a la sociedad humana en su conjunto. Desde la concentración de poder hasta las dinámicas globales, las disparidades de riqueza y las normas sociales, el sistema fiduciario influye directamente en cómo operan las naciones y cómo los ciudadanos comunes navegan sus vidas.

Actividad: Consecuencias del Sistema Fiat

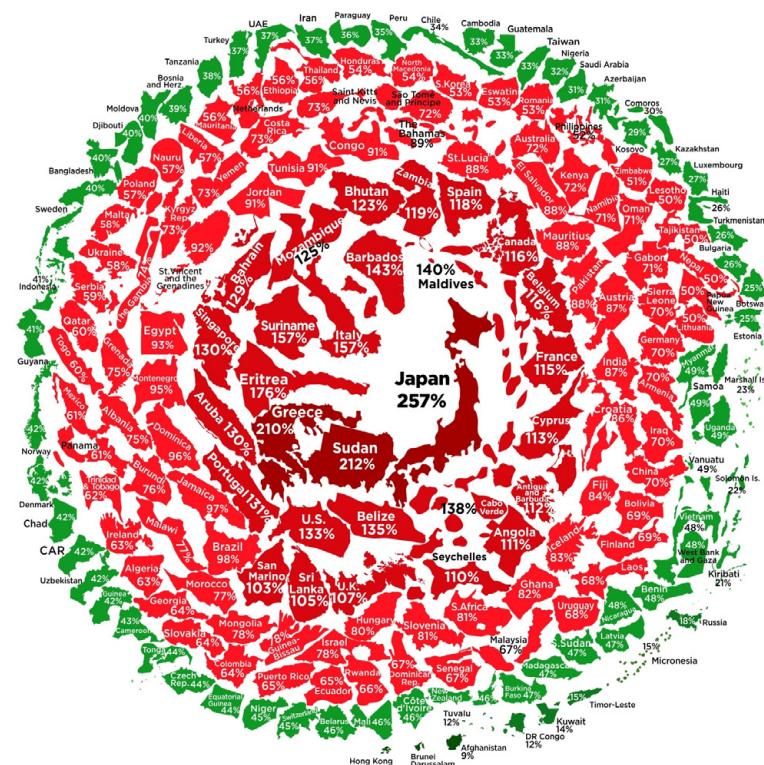
1. ¿Existen otras consecuencias que experimentan los individuos y la sociedad en su conjunto como resultado del sistema fiduciario?
2. Cuáles son las consecuencias en tu país como resultado del sistema fiduciario? ¿Qué ocurrió a lo largo de la historia y cómo afectó a la gente en tu país?
 - a. Ejemplos personales—sesión interactiva

5.2.3 La Carga Global de Deuda

Como resultado del sistema fiduciario, los gobiernos de todo el mundo se encuentran atrapados en una enorme red de deudas, atrapados en lo que se llama "la espiral global de deuda". Imagina un escenario en el que tomas prestado más dinero del que jamás podrás pagar. Esto está sucediendo a gran escala en todo el mundo. Los gobiernos, ahogados en deudas, se han visto atrapados en un peligroso juego de acumular más deuda de la que pueden pagar. Es una historia de gasto imprudente, endeudamiento y falta de previsión que ahora empuja a las naciones de todo el mundo al borde del desastre financiero.



A día de hoy, el gobierno federal de EE. UU. ha agregado una asombrosa cantidad de diez billones de dólares de nueva deuda desde 2019. La deuda total ha aumentado de alrededor de 23 billones de dólares durante el cuarto trimestre de 2019 a una astronómica cifra de 34 billones de dólares en la actualidad. La velocidad a la que los gobiernos generan nueva deuda no se está desacelerando; de hecho, está acelerando. Se proyecta que el año 2023 sea el año más aditivo en deuda desde los turbulentos tiempos de 2021, marcados por la pandemia de COVID.



Entonces, ¿qué significa esto para los individuos y las sociedades que ya necesitan lidiar con las consecuencias del sistema fiduciario? La espiral de deuda en la que están atrapados es como una bola de nieve rodando cuesta abajo, simplemente sigue creciendo y no estamos seguros de cómo detenerla. Las consecuencias mencionadas anteriormente, desde la desigualdad de riqueza hasta la agitación social, no desaparecerán. En cambio, la carga global de deuda ha alcanzado un punto sin retorno, asegurando que las cosas estén destinadas a empeorar.

Relación deuda/PIB 2021 (%)



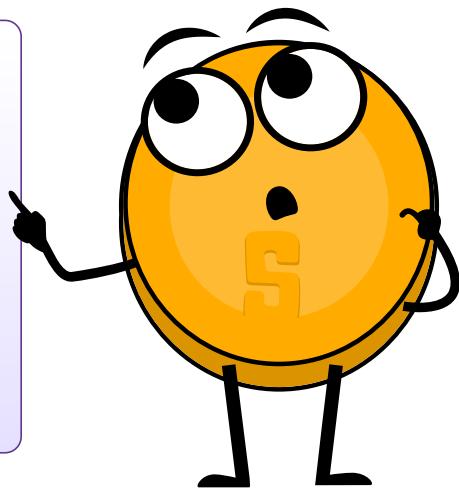
Cómo Los Problemas Conducen a Soluciones



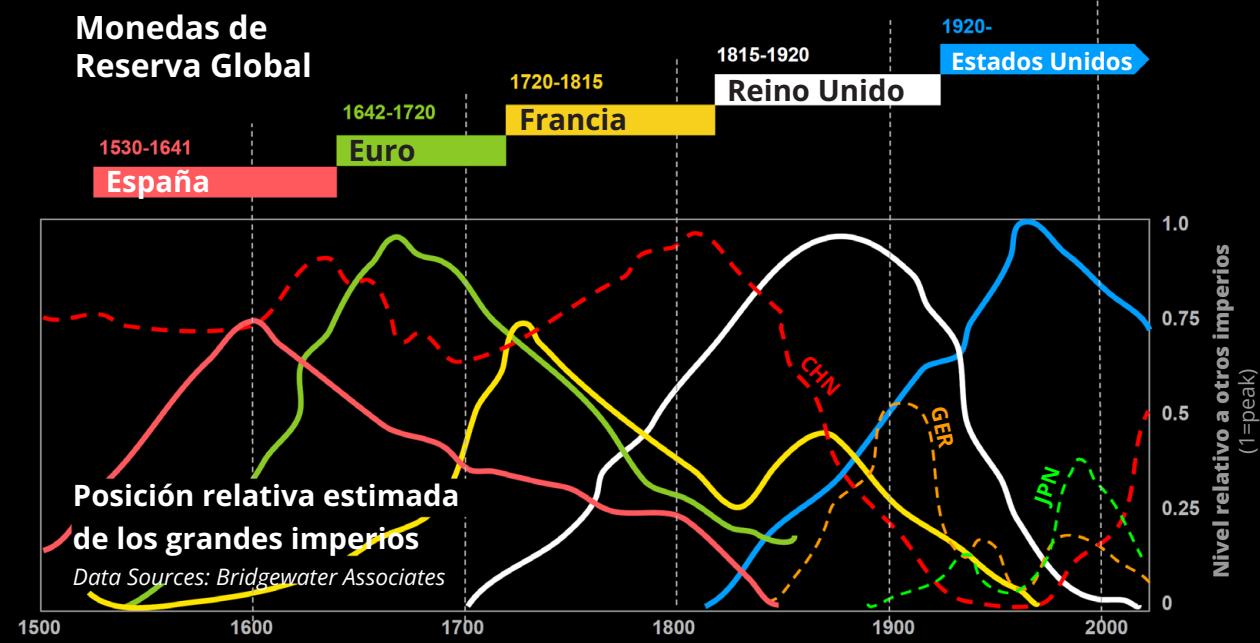
"No creo que volvamos a tener buen dinero hasta que le quitemos el asunto de las manos al gobierno... todo lo que podemos hacer es, de alguna manera astuta y indirecta, introducir algo que ellos no puedan detener."

Friedrich Hayek

Ganador Premio Nobel de Economía



Monedas de Reserva Global



5.3 Los Cypherpunks y la búsqueda de una moneda descentralizada

Hemos observado una captura progresiva del dinero por parte de bancos y gobiernos a lo largo de la historia, lo que ha llevado al sistema fiduciario que conocemos hoy en día, y sus desastrosas consecuencias para la sociedad. Pero el surgimiento de nuevas tecnologías como el cifrado y el internet permitió que surgieran nuevas ideas, como el dinero digital independiente, libre de intervención gubernamental, abierto y accesible para todos. Sumergámonos en el viaje de quienes lideran este movimiento revolucionario: los Cypherpunks.

5.3.1 Los Cypherpunks

La computadora puede ser usada como una herramienta para liberar y proteger a las personas, en lugar de controlarlas

Hal Finney

La segunda mitad del siglo XX vio el surgimiento de múltiples avances tecnológicos como la computadora y el internet, allanando el camino para una nueva era digital.

Un grupo de personas descubrió que estas enormes innovaciones pronto transformarían cómo funciona la sociedad. Anticiparon tanto el potencial como el peligro de la computadora personal, ya sea como una herramienta que permitiera la libertad para empoderar al individuo, o como una herramienta para un control y vigilancia completos.

Estas personas fueron llamadas los Cypherpunks. Surgieron como un grupo de activistas, criptógrafos, programadores y defensores de la privacidad conectados de manera informal que compartían una visión común: la búsqueda de privacidad, seguridad y un futuro digital descentralizado. El término "Cypherpunk" es una fusión de "cypher", refiriéndose a código criptográfico, y "punk", representando el ethos contracultural de rebelión.

Los Cypherpunks creían en el poder de la criptografía para proteger las libertades individuales. Sus objetivos incluían el desarrollo de herramientas para asegurar las comunicaciones en línea, anonimizar actividades en internet y establecer monedas digitales para operar más allá del control de autoridades centralizadas.

Los Cypherpunks entendieron las consecuencias del sistema fiduciario y vieron la amenaza de un "futuro orwelliano". Creían que tenían que asegurarse de que la computadora personal y el internet se convirtieran en algo bueno para la humanidad, en lugar de herramientas que pudieran exacerbar el control del Estado sobre el pueblo.

LA DEFINICIÓN DE UN FUTURO ORWELLIANO:

Un futuro orwelliano se refiere a una visión distópica inspirada en las obras de George Orwell. El término está asociado con una sociedad pesadillesca y totalitaria caracterizada por un control gubernamental opresivo, una vigilancia extensiva, propaganda y la manipulación de la información. El término "orwelliano" a menudo describe un escenario donde las libertades de los ciudadanos y la autonomía individual están severamente restringidas, la disidencia está suprimida y la realidad está distorsionada para servir a los intereses de un régimen poderoso y autoritario. El concepto lleva el nombre de George Orwell, quien, en sus escritos, advirtió sobre los peligros potenciales del poder gubernamental no controlado y la erosión de los derechos humanos fundamentales.



Cómo Los Problemas Conducen a Soluciones

Lore ipsum

Figuras clave dentro del movimiento Cypherpunk incluyeron luminarias como Eric Hughes, Timothy C. May y John Gilmore. En 1992, Eric Hughes redactó "Un Manifiesto Cypherpunk", delineando los principios del grupo. El manifiesto enfatizaba la importancia de la privacidad, la criptografía y la necesidad de que los individuos tomaran el control de sus identidades digitales.



Mira este video y descubre el manifiesto Cypherpunk por Eric Hughes!

Una de las invenciones más destacadas de los Cypherpunks fue la creación de herramientas y protocolos criptográficos. En 1991, Phil Zimmermann introdujo PGP (Pretty Good Privacy), un software de cifrado de correo electrónico que se convirtió en un proyecto emblemático. PGP permitió a los usuarios enviar mensajes cifrados por internet sin la capacidad de que nadie más que el destinatario previsto los descifrara. Antes de eso, cualquier mensaje enviado por internet podía ser interceptado y leído por otros, como los gobiernos.

Los Cypherpunks pensaron que el avance del cifrado, junto con el internet y la computadora, proporcionaba una base sólida para la creación de redes descentralizadas en el espacio digital, permitiendo que los individuos se comunicaran y realizaran transacciones en internet de manera privada y sin la interferencia de una autoridad central.

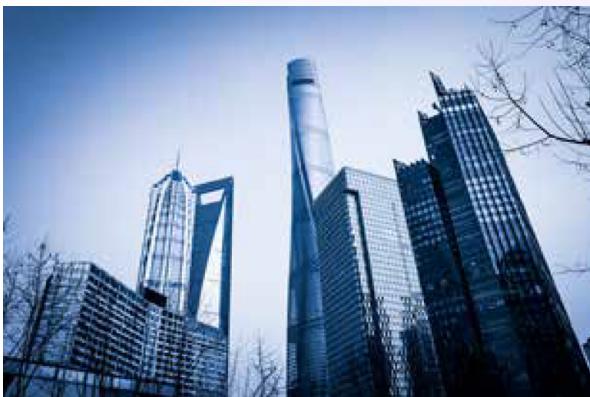
Los Cypherpunks estaban en el camino correcto para fomentar un futuro más brillante para la humanidad, donde la tecnología sería una herramienta para maximizar la libertad, en lugar de control. La única pieza que faltaba era una red descentralizada y una moneda digital descentralizada.

5.3.2 Sistemas Centralizados vs. Descentralizados

Sistemas Centralizados: Un Gobernante, Muchos Problemas

En un sistema centralizado, todo gira en torno a una autoridad principal, como un edificio alto en una ciudad. Esta autoridad controla cómo funciona todo el sistema. Piensa en los bancos tradicionales como ejemplo, donde un pequeño grupo toma todas las decisiones.

Ejemplo del mundo real: En 2022, durante protestas pacíficas en Canadá, los bancos congelaron las cuentas de los manifestantes, mostrando cómo la autoridad central podría intervenir y controlar el acceso financiero.



Problemas con los Sistemas Centralizados:

- 👉 Punto central de falla: Si algo sale mal con la autoridad central, todo el sistema puede colapsar.
- 👉 Control: Un pequeño grupo en la cima tiene mucho control y poder, a menudo tomando decisiones que los benefician más que a todos los demás
- 👉 Ineficiencia e Intermediarios: Como los atascos de tráfico en una ciudad, los sistemas centralizados pueden volverse lentos y costosos debido a intermediarios innecesarios.
- 👉 Falta de Autonomía: Las personas pueden no tener la oportunidad de tomar sus propias decisiones financieras; todo está decidido por la autoridad superior.
- 👉 Censura y Restricción: Al igual que algunas partes de una ciudad pueden ser bloqueadas, los sistemas centralizados pueden bloquear o limitar el acceso a ciertos recursos financieros.
- 👉 Desafíos de Escalado: Cuando más personas necesitan servicios financieros, los sistemas centralizados pueden tener dificultades para mantenerse al día.
- 👉 Riesgos de Seguridad: Los problemas con la autoridad central pueden poner en riesgo todo el sistema de ataques ciberneticos.
- 👉 Falta de Transparencia y Confianza: El funcionamiento interno de los sistemas centralizados puede ser difícil de entender, lo que dificulta que las personas confíen en ellos.

Sistemas Descentralizados: Poder para las Personas

Ahora, piensa en un sistema descentralizado como un gran bosque. Cada árbol representa una parte separada, y todo el bosque representa todo el sistema. A diferencia de una ciudad con un punto central único, un sistema descentralizado es más como un bosque resiliente que puede seguir adelante incluso si una parte enfrenta problemas.

- 👉 Ejemplo del mundo real: La Red Tor y su Navegador Tor crean un sistema descentralizado donde las personas pueden mantenerse anónimas en internet, y la red es difícil de detener o censurar.



Beneficios de los Sistemas Descentralizados:

- 👉 Resiliencia y Confiabilidad Mejoradas: No hay un solo punto de falla que haga al sistema fuerte, incluso si hay algunos problemas.
- 👉 Mayor Seguridad: Con la encriptación/protección adecuada, un sistema descentralizado es mejor para resistir el control de una sola autoridad.

Cómo Los Problemas Conducen a Soluciones

- 💡 Mayor soberanía: Las personas tienen más control sobre su dinero, datos y decisiones.
- 💡 Transparencia mejorada: Todos ven la misma información, lo que hace que el sistema sea más confiable.
- 💡 Naturaleza permisible e ilimitada: Cualquiera puede unirse o participar, lo que lo convierte en un sistema financiero inclusivo.
- 💡 Oportunidades iguales: Todos tienen una oportunidad justa de contribuir y tener voz.
- 💡 Privacidad mejorada: los datos se distribuyen entre múltiples participantes y son en su mayoría seudónimos, lo que hace que los sistemas descentralizados sean más privados.

Si bien los sistemas descentralizados tienen muchas ventajas, tomar decisiones juntos puede ser un poco complicado. Requiere que todos trabajen juntos.

Cambiando cómo se ejerce el poder

En el mundo de los sistemas centralizados y descentralizados, todo se trata de quién tiene el poder. Los sistemas centralizados otorgan poder a un pequeño grupo, mientras que los sistemas descentralizados lo distribuyen, permitiendo que todos tengan voz. Este cambio de poder significa un futuro financiero más justo y democrático, donde muchas personas influencian el sistema que da forma a sus vidas.

5.3.3 Breve Historia de las Monedas Digitales

Uno de los conceptos más cruciales discutidos por los Cypherpunks fue el dinero digital. Los Cypherpunks se dieron cuenta de que el estado y el dinero necesitaban separarse para asegurar que el futuro beneficiara al bien común. El trabajo innovador de David Chaum en protocolos criptográficos para transacciones seguras y privadas sentó las bases. La desventaja era que este protocolo requería una autoridad central para funcionar eficientemente, lo que planteaba preocupaciones sobre un punto único de falla y censura potencial.

En los años siguientes, varios Cypherpunks intentaron iterar las ideas de los demás para crear una solución viable para una moneda digital libre de control gubernamental. La tabla a continuación describe varias innovaciones clave que los Cypherpunks desarrollaron en su búsqueda por crear dinero digital:

Nombre y Fecha	Descripción	Limitaciones
E-Cash (1982)	El E-Cash de David Chaum fue un concepto temprano de dinero electrónico, enfocándose en la privacidad a través de técnicas criptográficas.	Requería de una autoridad central, lo que generaba preocupaciones sobre un único punto de falla y una posible censura.
DigiCash (1990)	DigiCash, fundada por David Chaum, tenía como objetivo crear una forma digital de moneda con énfasis en la privacidad.	El modelo centralizado contribuyó a su eventual quiebra en 1998.

Capítulo #5

B-Money (1996)	B-money, propuesto por Wei Dai, era una propuesta teórica para un sistema de efectivo electrónico distribuido y anónimo.	Nunca implementado, siendo una idea conceptual. Faltaba una implementación práctica.
HashCash (1998)	Hashcash, desarrollado por Adam Back, era un sistema de prueba de trabajo diseñado para limitar el spam de correo electrónico y los ataques de denegación de servicio.	No abordó directamente el problema del doble gasto asociado con las monedas digitales.
Bit Gold (1998)	Bit Gold, propuesto por Nick Szabo, describió un sistema de moneda digital descentralizado con elementos de prueba de trabajo.	Nunca implementado, siguió siendo un concepto teórico.
e-Gold (2004)	E-Gold era una moneda digital centralizada respaldada por oro físico, que permitía a los usuarios comprar y transferir unidades e-gold.	Problemas legales llevaron a su cierre en 2009, destacando los desafíos asociados con las monedas digitales centralizadas.

A pesar de los numerosos intentos realizados por los Cypherpunks durante décadas para crear una moneda digital libre del control de cualquier grupo o gobierno, sus esfuerzos enfrentaron desafíos prácticos y no pudieron materializarse completamente en el mundo real. Los Cypherpunks llegaron a la conclusión de que no era tan fácil crear una forma digital de efectivo que fuera segura, escalable y que tuviera el potencial de ser ampliamente adoptada.

Sin embargo, la historia da un giro cuando un individuo, aprendiendo de las lecciones de los Cypherpunks, eleva el concepto de moneda digital descentralizada a nuevas alturas. En los siguientes capítulos, exploraremos cómo la contribución de esta persona, basada en 40 años de trabajo previo, condujo en última instancia a la creación de un sistema funcional.

Capítulo #6

Una Introducción a Bitcoin

6.0 Satoshi Nakamoto y la creación de Bitcoin

6.1 ¿Cómo funciona Bitcoin?

6.1.1 El Mecanismo de Consenso de Nakamoto

6.1.2 Los Jugadores del Juego

Actividad: Construcción de Consenso en una Red Peer-to-Peer

6.2 Bitcoin como dinero digital sólido

6.2.1 Introducción

6.2.2 Características de Bitcoin

Actividad: Discusión en clase - ¿Es Bitcoin Dinero Sólido?

6.2.3 Aceptando la Responsabilidad Personal

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

Una Introducción a Bitcoin

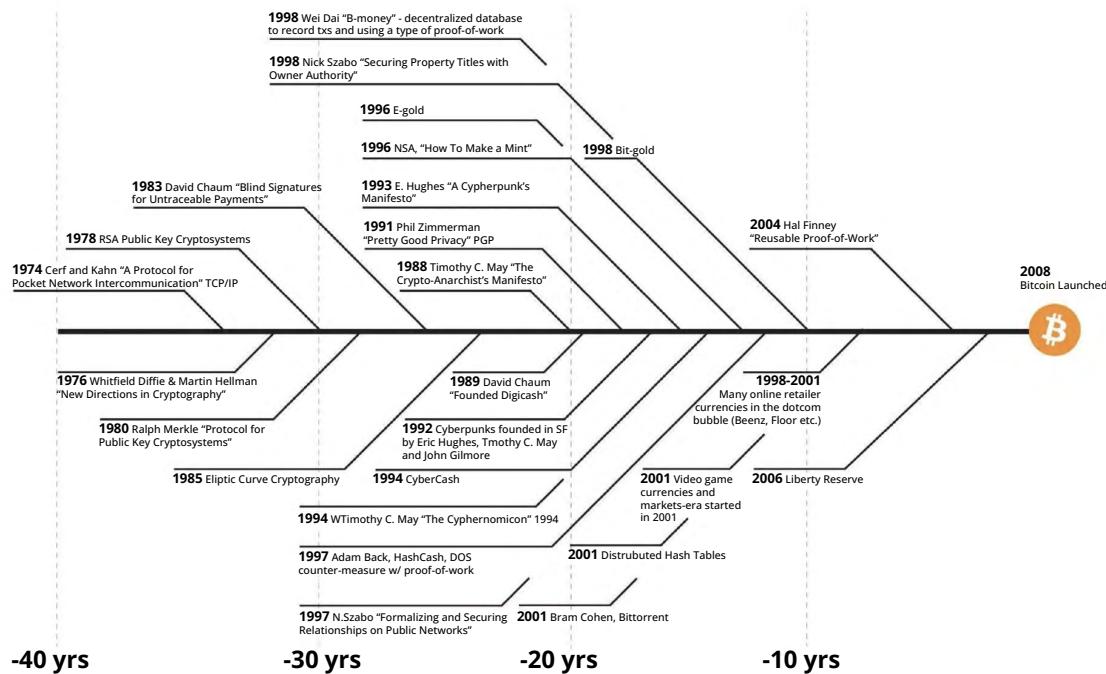
6.0 Satoshi Nakamoto y la Creación de Bitcoin

Muchas personas automáticamente descartan la moneda electrónica como una causa perdida debido a todas las empresas que fallaron desde la década de 1990.

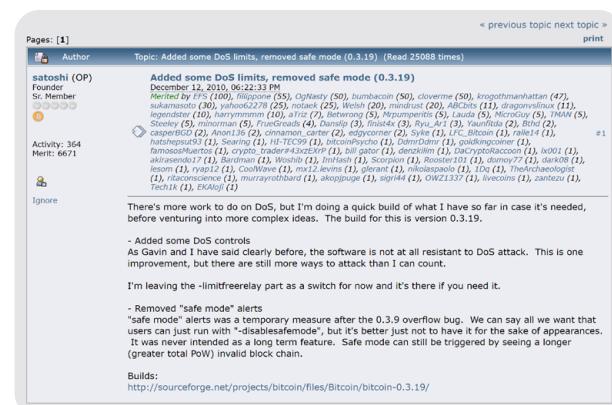
Espero que sea evidente que fue solo la naturaleza centralmente controlada de esos sistemas lo que los condenó. Creo que esta es la primera vez que estamos probando un sistema descentralizado no basado en confianza

Satoshi Nakamoto

Prehistoria de Bitcoin: — Es el resultado de 40 años de investigación, desarrollo y demanda.

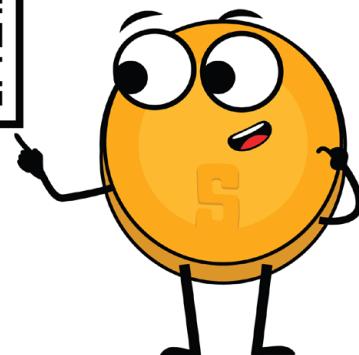


Como has leído en el capítulo anterior, varios Cypherpunks intentaron crear un sistema de dinero alternativo. Este capítulo continúa la historia de uno de ellos: una mente visionaria llamada "Satoshi Nakamoto". Esta persona anónima (hombre, mujer o grupo) había sido, mucho antes de Bitcoin, parte de entusiastas de la criptografía como científicos informáticos y hackers, participando en discusiones para encontrar soluciones prácticas que reemplazaran al sistema fiduciario.



Capítulo #6

En octubre de 2008, Nakamoto presentó un innovador whitepaper titulado 'Bitcoin: Un Sistema de Efectivo Electrónico Peer-to-Peer' en una lista de correo de criptografía. Este documento sentó las bases para un protocolo descentralizado peer-to-peer, diseñado para facilitar transacciones en línea seguras sin necesidad de intermediarios. La visión de Nakamoto era clara: crear una versión puramente peer-to-peer del efectivo electrónico, libre del control de gobiernos poderosos e instituciones financieras.



Avancemos rápidamente al 3 de enero de 2009, cuando Nakamoto minó el primer bloque de Bitcoin, conocido como el "bloque génesis". Esto marcó el lanzamiento oficial de la red Bitcoin, un nuevo sistema de dinero construido en confianza y seguridad a través de un libro contable descentralizado. En los meses y años siguientes, cada vez más entusiastas se unieron y contribuyeron a la idea.

Bitcoin Genesis Block

Raw Hex Version

.....
.....;ÍÍýz.;²cZ;
gv.a.Æ.Á°SQ2.Ý;
K.ºJ^y_IÝy.º+
.....
.....
.....;ÝÝÝM.ÝÝ;
..The Times 03
Jan/2009 Chance
lor on brink of
second bailout
or banksyyyyy..ó
*****.CA.g§yþPUH
....ñ|q'w.ºÖ.º(º.º
ybæ.ºabºtöº?Li8
ðú.ºA.ºD.BMº*º
Sñ+rñh ..

En 2011, después de que la red Bitcoin demostrara que podía operar con éxito sin la necesidad de su influyente creador, Nakamoto envió un correo electrónico a un compañero desarrollador de Bitcoin, anunciando su retiro de la escena de Bitcoin y cediendo su futuro a otras "buenas manos" que compartieran su visión.

Aunque la identidad de Nakamoto sigue siendo un misterio hasta el día de hoy, su objetivo al crear Bitcoin nunca fue un misterio. En esencia, Nakamoto lo creó para quitar el poder de unos pocos y devolvérselo a muchos, creando una alternativa en forma de un sistema monetario descentralizado, de código abierto y transparente, separando el dinero del estado. La creación de Bitcoin fue la respuesta de Nakamoto a la crisis financiera de 2008 que perjudicó a personas comunes en todo el mundo mientras enriquecía a la élite, Bitcoin fue la respuesta de Nakamoto a la corrupción y fragilidad del sistema fiduciario. Nakamoto sentó las bases para una nueva revolución y se alejó en lugar de reclamar crédito.

Una Introducción a Bitcoin

En los años siguientes, Bitcoin comenzó a crecer rápidamente y se convirtió en un símbolo de esperanza, empoderamiento y resistencia, desafiando el sistema fiduciario y proporcionando un medio seguro y resistente a la censura para transacciones financieras. Bitcoin es un protocolo de código abierto, lo que significa que nadie tiene el poder de poseerlo o controlarlo. Su diseño es público y está abierto para que cualquiera participe.

Hoy en día, el sueño de Nakamoto de un sistema financiero transparente y seguro sin fronteras sigue vivo, impulsando la revolución global de la libertad que presenciamos hoy. Todos los días, personas comunes optan por salir del sistema fiduciario y unirse al mundo de Bitcoin. Se han creado centros de Bitcoin, las llamadas economías circulares de Bitcoin, por entusiastas de la libertad en pueblos de todo el mundo. Incluso países enteros que buscan una alternativa, como El Salvador, están comenzando a adoptar Bitcoin a su manera.

6.1 ¿Cómo Funciona Bitcoin?

6.1.1 El Mecanismo de Consenso de Nakamoto

Entonces, ¿cómo funciona Bitcoin? Bitcoin tiene muchas características y la madriguera del conejo es muy profunda.

Afortunadamente, si entras en el mundo de Bitcoin por primera vez, no es necesario entender perfectamente cómo funciona para empezar a usarlo. Lo mismo ocurre con el uso de Internet. La mayoría de las personas no saben cómo funciona el protocolo TCP/IP, pero aún envían correos electrónicos, mensajes y publican contenido en sus redes sociales todos los días. Lo mismo ocurre al conducir un automóvil. La mayoría de las personas no saben exactamente cómo funciona un automóvil, pero saben cómo conducir.



Sin embargo, Bitcoin aún no se ha adoptado ampliamente. Es una tecnología bastante nueva, como lo fue Internet durante los años 90. Debido a eso, puede ser útil entender lo básico de Bitcoin de manera simple y menos técnica.

Capítulo #6

La idea clave detrás de cómo opera Bitcoin se puede resumir en una frase: Bitcoin es un acuerdo entre personas en línea. Puedes pensarla como jugar un juego de mesa con amigos. Cuando juegas un juego de mesa como Monopoly, estás de acuerdo con los otros jugadores sobre reglas específicas. Una de las reglas de Monopoly es que solo se aceptarán "billetes de Monopoly" especiales. Si James, uno de los jugadores, va en contra de las reglas al usar papel higiénico para comprar una casa en lugar de billetes de Monopoly, los demás jugadores le dirían a James que está haciendo trampa y simplemente dejarían de jugar con él. En resumen, para jugar el juego, hay consenso sobre un conjunto de reglas entre ustedes, y no se apartan de esas reglas, de lo contrario, serán rechazados.

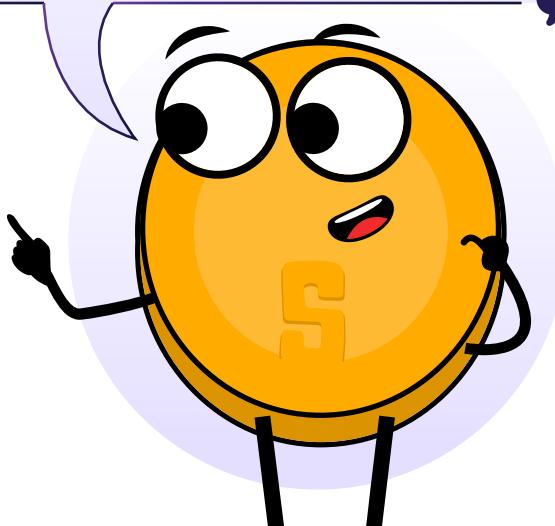
Básicamente, así es como funciona Bitcoin. Bitcoin es una red de personas que están de acuerdo con el mismo conjunto de reglas. Estas reglas están vinculadas matemáticamente, escritas en código informático y aceptadas directamente por todas las personas que ejecutan el software de Bitcoin. Las reglas de Bitcoin se aplican a todos los participantes por igual, lo que significa que todos siguen las reglas del juego o no pueden jugar porque serán rechazados por la red.

Por ejemplo, una de las reglas es "Nunca habrá más de 21 millones de tokens de bitcoin". Si algunas personas quieren crear 1 millón de bitcoins adicionales para sí mismas, no les servirá de nada, porque automáticamente serían identificados y rechazados por todos los demás. Esto es lo que hace que Bitcoin sea tan robusto.

No importa quién seas ni de dónde vengas, si entras en el mundo de Bitcoin, debes jugar con el mismo conjunto de reglas que cualquier otra persona.

Esto también se aplica a todas las personas y entidades que tenían un gran control e influencia en el mundo fiduciario. En el mundo de Bitcoin no hay lugar para hacer trampa o sabotaje. Todos son tratados por igual y nadie puede cambiar eso.

¿Sabías que, desde 2009, Bitcoin ha resistido decenas de miles de intentos de piratearlo, manipularlo o alterarlo? Bitcoin demostró que nadie puede detenerlo, controlarlo o manipularlo.



Una Introducción a Bitcoin

6.1.2 Los Jugadores del Juego

Para comprender mejor la descentralización de Bitcoin, necesitamos sumergirnos en los diferentes roles dentro de la red. En el mundo de Bitcoin, varios participantes desempeñan roles distintos pero armónicos, contribuyendo al funcionamiento sin problemas de la red.

1. Mineros: Los Arquitectos de la Seguridad

Los mineros son la columna vertebral de Bitcoin. Estas son personas o grupos de personas que trabajan detrás de escena para mantener y asegurar la red mediante un mecanismo llamado Prueba de Trabajo (PoW). Estos jugadores están equipados con computadoras especiales que contienen una gran potencia computacional. Ponen sus equipos a disposición de la red Bitcoin para competir entre ellos y encontrar números criptográficos complejos, verificando transacciones y añadiendo nuevos bloques de información sobre transacciones al libro contable descentralizado de Bitcoin (llamado blockchain). Su compromiso garantiza la inmutabilidad del libro contable y protege contra ataques maliciosos.

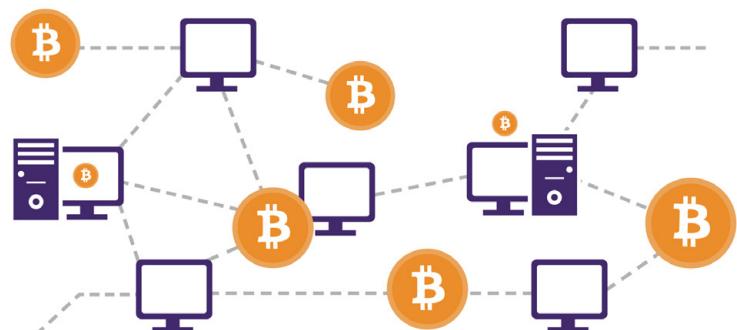


La naturaleza descentralizada de la minería permite que cualquier persona con recursos computacionales suficientes participe. Gracias a su arduo trabajo, los mineros que resuelven el rompecabezas más rápido son recompensados en forma de Bitcoin.

Los mineros de Bitcoin están distribuidos por todo el mundo, protegiendo la red contra la centralización y asegurando que la seguridad de Bitcoin se mantenga robusta y distribuida.

2. Nodos: Guardianes de la Validación

Los Nodos de Bitcoin son personas comunes que viven en todo el planeta. Estos participantes forman los guardianes de la red Bitcoin ejecutando el software de Bitcoin en sus pequeñas computadoras, en las cuales mantienen una copia del libro contable completo. Los nodos validan transacciones y aseguran que todos los participantes sigan las reglas de consenso.



Al distribuir la responsabilidad de la validación en una red de nodos, Bitcoin sigue siendo resistente contra ataques y mantiene su naturaleza sin confianza. Los nodos desempeñan un papel crucial en mantener la integridad del libro contable, contribuyendo a la ética de descentralización de Bitcoin.

3. Usuarios: Participantes Empoderados

Los usuarios, la fuerza vital de la red Bitcoin, son individuos que participan en transacciones. Puedes pensar en los usuarios como personas comunes que simplemente viven sus vidas, pero que también se han empoderado al integrar Bitcoin de alguna manera. Por ejemplo, algunos usuarios guardan su dinero en Bitcoin. Otros, como los ciudadanos de El Salvador, usan Bitcoin como dinero para comprar alimentos y reciben Bitcoin en forma de salario.

Bitcoin empodera a los usuarios eliminando la necesidad de intermediarios como bancos y gobiernos, permitiendo transacciones directas peer-to-peer. Esto también significa que los usuarios tienen control total sobre su dinero, proporcionando autonomía sobre sus fondos y transacciones.

4. Desarrolladores y Proyectos: Arquitectos de la Innovación

El sistema monetario del futuro no se construye solo ni logra una adopción global de manera éticamente correcta sin esfuerzo. Aquí es donde entran en juego los desarrolladores de Bitcoin y los proyectos de Bitcoin.

Los desarrolladores utilizan su experiencia técnica para mejorar e innovar el protocolo de Bitcoin. Estas personas contribuyen con código, proponen mejoras y abordan vulnerabilidades, asegurando que la red evolucione en respuesta a todo tipo de desafíos. La naturaleza de código abierto de Bitcoin invita a la colaboración, permitiendo que desarrolladores de todo el mundo contribuyan a su crecimiento.

La belleza de este desarrollo descentralizado evita que una sola entidad monopolice el control sobre el protocolo. Esto ocurre a través de un proceso impulsado por el consenso. Los desarrolladores proponen ideas y cambios, y solo aquellos con las mejores ideas alineadas con la visión más amplia de un mundo mejor reciben el respaldo de la comunidad, potenciando una evolución transparente y democrática de Bitcoin hasta que esté listo para 8 mil millones de personas.

Los proyectos de Bitcoin involucran a grupos diversos, desde organizaciones sin fines de lucro con una misión, hasta corporaciones, grupos e individuos que crean contenido valioso, entre otros. Estas son personas que trabajan juntas en un objetivo o enfoque específico dentro de la misión más grande de Bitcoin hacia la libertad colectiva.

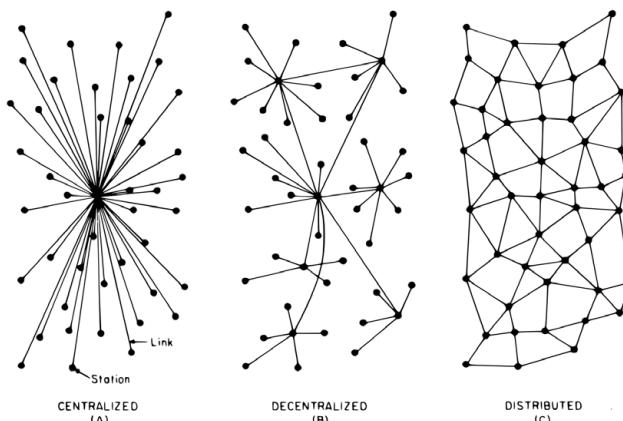
Una Introducción a Bitcoin

La Sinfonía

La descentralización de Bitcoin se puede pensar como una sinfonía orquestal sinérgica, un acto de equilibrio donde todos los diferentes jugadores de instrumentos crean la música más hermosa juntos. No hay un jefe en la red Bitcoin, en cambio, tanto los mineros, nodos, usuarios, desarrolladores y proyectos realizan sus roles con autonomía y colaboración. El libro contable descentralizado, mantenido por nodos, garantiza la transparencia, mientras que el mecanismo de prueba de trabajo proporciona seguridad y disuade la centralización en la minería. Los usuarios experimentan la soberanía financiera y el empoderamiento, libres del control del sistema fiduciario. Los desarrolladores, guiados por el consenso, aseguran que el protocolo se adapte a las necesidades cambiantes de la humanidad. Los proyectos de Bitcoin, de maneras únicas, contribuyen a la misión más amplia de la libertad colectiva.

Como puedes ver, cada participante juega un papel vital en la adopción de Bitcoin y en el empoderamiento de la humanidad. Cada participante en esta orquesta descentralizada contribuye a la resistencia y longevidad de Bitcoin, creando un ecosistema sin confianza, sin fronteras y empoderador.

En resumen, la sinfonía de descentralización en Bitcoin resuena como un testimonio de la visión de Satoshi Nakamoto y la inmensa pasión de una comunidad global en busca de libertad y empoderamiento.



Actividad en Clase — Construcción de Consenso en una Red Peer-to-Peer

Objetivo



Comprender cómo se logra el consenso en un grupo, aprender sobre criptografía y la capa de consenso de Bitcoin.

Materiales



Mensaje con instrucciones encriptadas y sin encriptar para acciones ("atacar" o "no atacar").

Preparación de la actividad

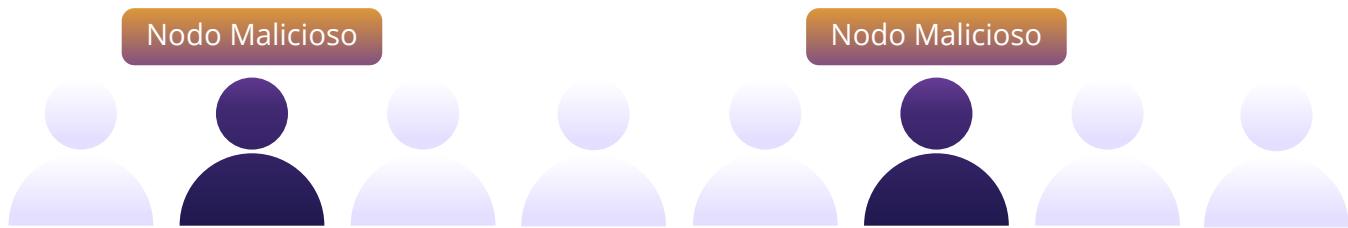


El maestro seleccionará un grupo de tres o cuatro estudiantes antes de la clase para ser nodos maliciosos en la siguiente actividad. El maestro asignará a estos nodos maliciosos un rompecabezas criptográfico como tarea en la clase anterior.

Pasos del ejercicio:

1 El maestro seleccionará un "originador" que recibirá un mensaje en un trozo de papel que dice "ATAQUE" y una serie de números que dice "4-16-14-21-1-21-21-1-3-11-" a un estudiante del grupo.

2 Los estudiantes formarán un círculo en el espacio designado, asegurándose de que los estudiantes seleccionados que serán nodos maliciosos estén separados para mejorar la efectividad de la lección.



3 Una vez que el grupo haya formado un círculo, el originador pasará la nota al individuo del lado derecho del círculo.

4 Despues de que todos hayan leido el mensaje, el originador dará la señal al grupo diciendo "Ahora" y el grupo reaccionará al mensaje simultáneamente. Si el mensaje dice "ATAQUE", entonces todos los participantes darán un paso adelante.

5 Despues de la reacción inicial, algunos estudiantes (los que recibieron el mensaje encriptado e interpretaron correctamente) permanecerán quietos, mientras que el resto seguirá la instrucción original, revelando una falta de consenso.

Conclusión:

Discutir por qué no se logró el consenso, introduciendo el concepto del Problema de los Generales Bizantinos, cómo se relaciona con la necesidad de un objetivo común y luego discutiendo cómo Bitcoin proporciona una solución a este problema.

Una Introducción a Bitcoin

6.2 Bitcoin Como Dinero Digital Sólido

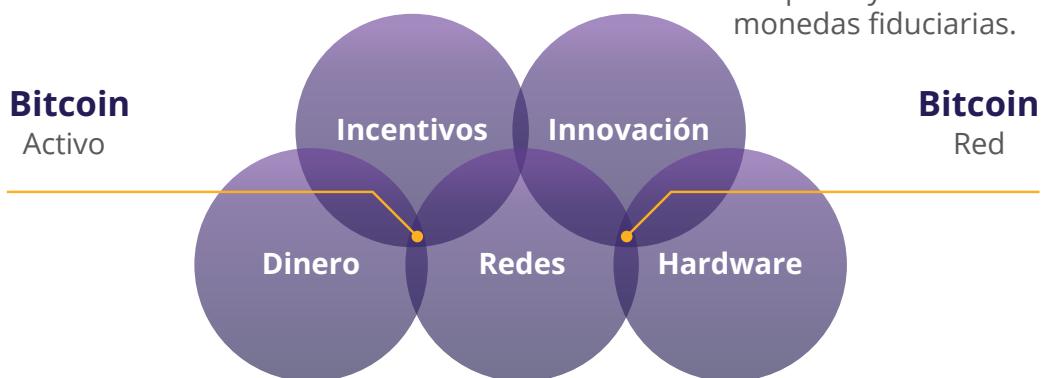
6.2.1 Introducción

Actividad:

Ver video de 1.5 minutos
"¿Qué es Bitcoin?"



En términos simples, Bitcoin es dinero. Bitcoin no es una inversión, sino más bien una forma segura y empoderadora de guardar tu dinero duramente ganado. Tener Bitcoin no significa que te hará rico, porque no te dará un rendimiento en más bitcoins. Su valor medido contra una moneda fiduciaria sí aumenta, pero esto se debe únicamente a su creciente adopción y la devaluación de las monedas fiduciarias.



Bitcoin es una nueva forma de dinero, es "El Internet del Dinero", lo que significa que Bitcoin está abierto para que cualquier persona se una y comience a intercambiar valor con otros usuarios de Bitcoin. Incluso las comunidades más aisladas y empobrecidas del mundo finalmente tienen acceso a un sistema monetario. Al igual que cualquier persona con un teléfono y una conexión a Internet puede usar un buscador, Bitcoin hace posible que todos aquellos con un teléfono y conexión a Internet accedan a un nuevo sistema monetario global.



Pagos más rápidos y más baratos

Envía dinero a todo el mundo en minutos, con tarifas extremadamente bajas



Inclusión Financiera

2.500 millones de personas no bancarizadas pueden tener acceso al dinero a través de un teléfono o una computadora.

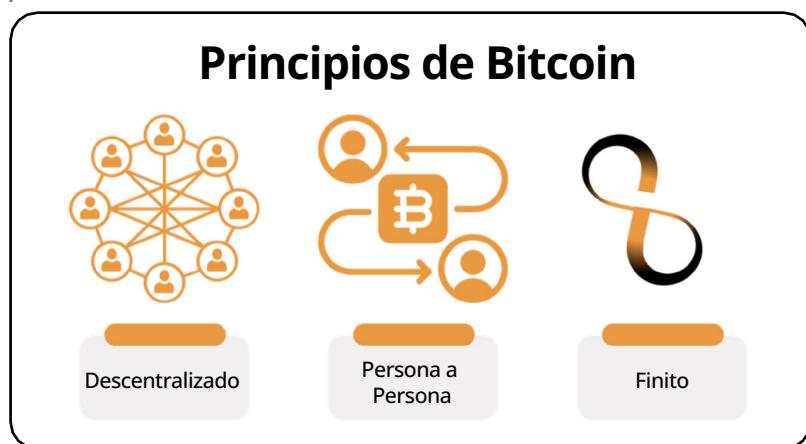


Mayor Privacidad

Las transacciones de Bitcoin son públicas pero tú identidad no lo es.

Bitcoin es completamente digital y sin fronteras. No importa dónde te encuentres, porque reside en computadoras y teléfonos inteligentes de personas distribuidas por todo el mundo. Muchos usuarios de todo el mundo ejecutan el software de Bitcoin y una copia de su libro contable. Este software y el registro de todas las transacciones tienen una probabilidad muy baja de desaparecer, ya que existen innumerables copias de él. Para cerrarlo, sería necesario apagar todo Internet para siempre, lo cual es altamente improbable.

Y finalmente, Bitcoin es escaso, lo que significa que la cantidad de tokens de bitcoin que pueden existir está absolutamente limitada. Nadie puede falsificar bitcoin, ni siquiera los gobiernos y las instituciones financieras más poderosas.



6.2.2 Características de Bitcoin

La Evolución del Dinero Sólido

Como has aprendido en el capítulo 2, el ciclo de vida del dinero sólido progresa a través de tres etapas para obtener aceptación general en la sociedad humana: desde ser una Reserva de Valor, hasta convertirse en un Medio de Intercambio, y finalmente, en una Unidad de Cuenta.

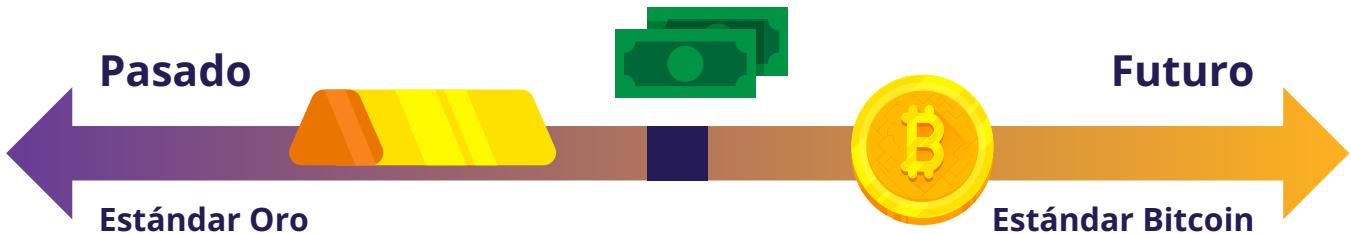
La primera etapa del dinero, siendo una Reserva de Valor, es cuando una moneda comienza a ganar confianza como un activo estable (o apreciable) con el tiempo. Aquellas personas que reconocen esto temprano buscan proteger su riqueza almacenándola en esta forma de dinero, especialmente durante momentos de incertidumbre geopolítica y macroeconómica.

Algunos grupos, como los medios de comunicación, llaman a Bitcoin una forma de "oro digital". Esto se debe a que Bitcoin se ha establecido firmemente como una reserva de valor durante la última década. Cada vez más personas comienzan a ver bitcoin como una protección contra la inflación, similar a como lo hizo el oro a lo largo de la historia humana.

La siguiente etapa es cuando la confianza en la estabilidad de una moneda se solidifica. Es en este momento que la moneda se convierte en un medio de intercambio, facilitando transacciones en la vida cotidiana de las personas. Durante esta etapa, comienza a ser ampliamente aceptada para el intercambio de bienes y servicios.

Bitcoin avanza progresivamente hacia convertirse en un medio de intercambio. Con la creciente aceptación por parte de comerciantes y el desarrollo del protocolo, las transacciones de Bitcoin se vuelven más eficientes y comunes en el comercio diario. Un ejemplo de esto es El Salvador, donde Bitcoin es reconocido oficialmente como moneda de curso legal. Cada día más ciudadanos comunes y negocios comienzan a usar Bitcoin como medio de intercambio.

Una Introducción a Bitcoin



En la etapa final, una moneda alcanza el estatus de unidad de cuenta, sirviendo como una medida común para fijar precios de bienes y servicios. Esta es la etapa en la que se convierte en la métrica estándar contra la cual se evalúan todos los demás valores.

El camino hacia convertirse en una unidad de cuenta es un proceso más prolongado (a largo plazo). Actualmente, el mundo mide bienes y servicios solo en monedas fiduciarias, y debido a eso, Bitcoin necesita una adopción más amplia e integración en varios sistemas financieros. Sin embargo, ya se ha sentado la base a medida que empresas e individuos comienzan a considerar y denominar valores en Bitcoin.



Como puedes ver, Bitcoin está bien encaminado en este ciclo evolutivo del dinero sólido. Cuando Bitcoin se integre completamente en el sistema financiero global, podría convertirse en una unidad estándar de cuenta, remoldeando todo el sistema monetario global.



Capítulo #6

Propiedades del dinero

Como has aprendido en el capítulo 2, la humanidad ha descubierto con el tiempo que el dinero sólido real debe poseer ciertas propiedades para ser efectivo. Estas propiedades son durabilidad, divisibilidad, portabilidad, aceptabilidad, escasez y fungibilidad.

Veamos si Bitcoin pasa la prueba.

Durabilidad: Bitcoin es completamente duradero al ser puramente digital.

Divisibilidad: Para comparación, la moneda fiduciaria USD puede dividirse hasta el centavo (.01). Bitcoin puede dividirse en lo que se conoce como un satoshi o sat (.00000001). Y debido al carácter digital de Bitcoin, incluso podría dividirse aún más en el futuro si la humanidad lo necesita. Bitcoin es actualmente el activo monetario más divisible del mundo.

Portabilidad: En abril de 2020, se transfirieron \$1.1 mil millones en solo unos minutos, y solo costó 68 centavos. Ninguna otra forma de pago puede mover tanta cantidad de dinero, a tan bajo costo, tan rápido y por sí sola. Esto es lo que hace que Bitcoin sea la forma de dinero más fácilmente móvil en el mundo.

Aceptabilidad: Bitcoin todavía está en sus primeras etapas de convertirse en un medio de intercambio, y en comparación con las monedas fiduciarias, la aceptabilidad de Bitcoin es actualmente baja.

Escasez: Solo habrá 21 millones de bitcoins en existencia. Es, por código, imposible que esta cantidad aumente, lo que significa que Bitcoin no solo es escaso, sino el activo monetario más escaso del mundo.

Fungibilidad: Cada unidad de bitcoin es igual a cualquier otra unidad de bitcoin y puede intercambiarse y transaccionarse a través del protocolo Bitcoin en una base de igualdad, lo que lo convierte en una moneda fungible.

Una Introducción a Bitcoin

Bitcoin vs. Oro vs. El dólar Estadounidense

Propiedades del Dinero	Oro	Fiat	Bitcoin
Durabilidad	Alta	Moderada	Alta
Portabilidad	Moderada	Alta	Alta
Divisibilidad	Moderada	Moderada	Alta
Fungibilidad	Alta	Alta	Alta
Escases	Moderada	Baja	Alta
Verifiable	Moderada	Moderada	Alta
Historia establecida	Alta	Moderada	Baja
Resistente a la censura	Moderada	Moderada	Alta
Inteligente/Programable	Baja	Moderada	Alta

*Bitcoin vs Oro vs El dólar Estadounidense" Bitcoin Magazine,

Bitcoin es un tipo de dinero inteligente que es programable, no puede ser confiscado y tiene todas las cualidades que lo hacen excelente para ahorrar y fácil para los comerciantes que desean transacciones rápidas. Dado que es un libro contable digital transparente, Bitcoin puede ser súper eficiente en cosas como detectar fraudes y calcular riesgos en sus servicios. Tiene las buenas partes del oro, como que solo hay una cantidad limitada de él, pero también tiene los beneficios de las monedas fiduciarias porque puedes dividirlo y llevártalo fácilmente contigo. Además, introduce nuevas características que funcionan bien en nuestro mundo digital.

¿Qué opinas? Aunque Bitcoin aún no es ampliamente reconocido y adoptado, ¿es Bitcoin un dinero sólido?

Actividad: Debate en clase - ¿Es Bitcoin un dinero sólido?

Ahora que hemos discutido Bitcoin con mayor detalle, volvamos a mirar nuestra tabla de comparación de dinero del Capítulo 2 y veamos cómo se compara Bitcoin con otras formas de dinero:

Características de buen dinero	VACAS	CIGARRILLOS	DIAMANTES	EUROS	BITCOIN
Durable					
Portable					
Uniforme					
Aceptable					
Escaso					
Divisible					
Total					

6.2.3 Aceptando la Responsabilidad Personal

El resultado es un sistema distribuido sin un solo punto de falla. Los usuarios tienen las claves criptográficas de su propio dinero y realizan transacciones directamente entre sí, con la ayuda de la red P2P para verificar el doble gasto.

Satoshi Nakamoto

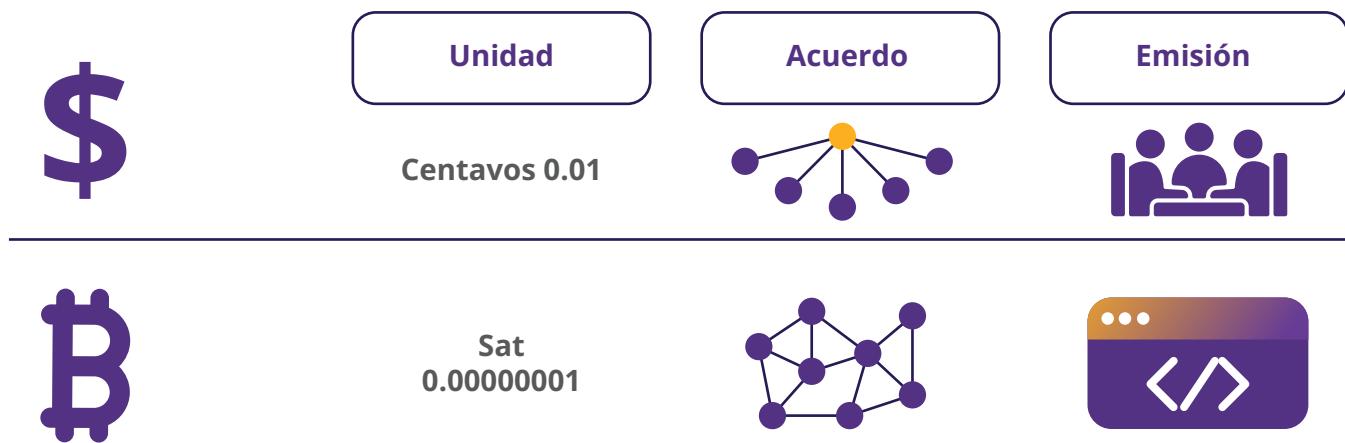
Una Introducción a Bitcoin

En el mundo fiduciario, la gente confía en los gobiernos, los bancos y los proveedores de pago establecidos. Los líderes de estas instituciones financieras establecen las reglas de la red, y los participantes, en su mayoría ciudadanos comunes, deben cumplir con estas reglas. No importa dónde vivas, siempre hay un conjunto de procedimientos estándar que te indican qué hacer y cómo hacerlo. Con el tiempo, esto llevó a un ciclo de dificultades, especialmente para las familias que luchan con los crecientes desafíos de la vida diaria.

Debido a este sistema, las personas están acostumbradas a poner la responsabilidad de sus finanzas en manos de otros. Por ejemplo, la mayoría de las personas dependen de otra persona para que las ayude, especialmente cuando algo sale mal (como perder el acceso a tu cuenta bancaria).



El sistema monetario de Bitcoin es, como sabes, muy diferente. Bitcoin opera de una manera específica y los gobernantes han sido reemplazados por un sistema autónomo de reglas. No hay dictador ni líder, lo que también significa que no hay nadie que te vaya a dictar qué debes hacer. Si deseas la libertad y el empoderamiento recién descubiertos de Bitcoin, tendrás que aprender cómo funciona e integrar la tecnología de una manera que funcione personalmente para ti.



Capítulo #6

Con Bitcoin, tienes el control total sobre tus fondos, pero con este control adicional también viene una responsabilidad aumentada. Por ejemplo, perder el acceso a tus Bitcoin al perder las claves de tu billetera digital significa que perdiste tus ahorros de manera permanente. No hay una línea directa de servicio al cliente a la que llamar o alguien más a quien acudir cuando hay un problema. Tienes que encargarte tú mismo.

Afortunadamente, esto no le sucederá a las personas que decidan asumir la plena responsabilidad sobre sus propias vidas. Usar Bitcoin no es inherentemente complicado; es solo un concepto nuevo. Cualquier incomodidad surge porque es desconocido, pero si estás dispuesto a aprender a usar Bitcoin y a abrazar completamente la responsabilidad de salvaguardar tu riqueza, Bitcoin se convierte en una herramienta poderosa, porque estás en control y nadie puede confiscar tu riqueza.

En resumen, la clave radica en la acción y en comprender el funcionamiento de Bitcoin e implementarlo de acuerdo con tus necesidades y filosofía de vida únicas. A continuación, comenzaremos a usar Bitcoin configurando una billetera de Bitcoin, enviando y recibiendo nuestras primeras transacciones, y revisando las mejores prácticas de seguridad.

Capítulo #7

Cómo Utilizar Bitcoin

7.0 Introducción

7.1 Adquisición e intercambio de Bitcoin

7.1.1 P2P: físico

7.1.2 Intercambios P2P: en línea

7.1.3 Plataformas de intercambios centralizados

7.2 Una introducción a las carteras de Bitcoin

7.2.1 Carteras auto custodiadas vs. custodiadas por terceros

7.2.2 Diferentes tipos de carteras de Bitcoin

7.2.3 Código abierto vs. código cerrado

Actividad - Evaluación en clase de las carteras de Bitcoin

7.3 Configuración de una cartera de Bitcoin móvil

Actividad - Configuración/recuperación de una cartera de Bitcoin

7.4 Recepción y envío de transacciones

Actividad - Transacciones de Bitcoin en acción

7.5 Ahorro en Bitcoin

7.6 No confíes, verifica

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

Cómo Utilizar Bitcoin

7.0 Introducción



¿Por qué alguien confiaría en dinero nerd en lugar de dinero del banco central?
Los nerds te trajeron Internet. Los bancos te trajeron la Gran Depresión.

Andreas M. Antonopoulos



Ahora que tenemos una mejor comprensión de qué es Bitcoin y su propósito, es hora de aprender cómo usarlo en la práctica. En este capítulo, te guiaremos paso a paso a través del proceso de adquisición de Bitcoin, exploraremos los diversos tipos de monederos disponibles, te ayudaremos a configurar tu propio monedero de Bitcoin e incluso practicaremos el envío y seguimiento de una transacción de Bitcoin en la red. ¡Es hora de convertir tu comprensión en acción!

7.1 Adquisición e intercambio de bitcoin

Existen muchas formas de adquirir bitcoin. Por ejemplo, puedes:

- ◆ Recibir pago en Bitcoin a cambio de tu trabajo y pagar productos y servicios de otras personas con bitcoin. (más sobre esto en el Capítulo 8)
- ◆ Minar Bitcoin (más sobre esto en el Capítulo 9)
- ◆ Intercambiar tu moneda fiduciaria por bitcoin o intercambiar tu bitcoin por moneda fiduciaria en persona.
- ◆ Intercambiar tu moneda fiduciaria por bitcoin o intercambiar tu bitcoin por moneda fiduciaria en línea.



A continuación, exploraremos el intercambio de moneda fiduciaria por bitcoin y viceversa, tanto a través de transacciones en persona como de métodos en línea, ya que son las opciones más comunes.

7.1.1 Entre pares en persona

Participar en transacciones entre pares (P2P) para adquirir y vender bitcoin implica intercambiar directamente tu moneda fiduciaria (o cualquier otro bien o servicio) por bitcoin con otra persona, eliminando la necesidad de que un banco u otra parte participe en la transacción.

Ambas partes determinan mutuamente la cantidad y la tasa de intercambio. El comprador proporciona el efectivo, el vendedor transfiere el bitcoin y la transacción concluye. Aunque es más fácil realizar intercambios P2P físicamente al reunirse con la otra persona directamente en el mundo real, también puedes hacerlo virtualmente desde cualquier lugar, gracias a Internet. Además, el intercambio de bitcoin por moneda fiduciaria sigue un proceso similar en sentido inverso.



7.1.2 Entre pares en línea

Ingresá a las plataformas P2P, donde los compradores y vendedores de Bitcoin se encuentran en el ciberespacio para realizar transacciones sin intermediarios, directamente en Internet.

Con estas plataformas, no tienes que confiar en nadie con tu información o tu dinero, puedes encontrarte con otros pares y comerciar con ellos directamente.



En la mayoría de las plataformas P2P, los pares deben depositar parte de los fondos en garantía para asegurarse de que cumplirán con su parte del trato. La garantía significa poner el dinero en un lugar seguro que la plataforma controla hasta que ambas partes cumplan con lo prometido. Es como tener a un amigo de confianza que cuida tus cosas hasta que todos cumplan su palabra.

7.1.3 Intercambios centralizados

Utilizar intercambios centralizados puede ser la forma más fácil de adquirir y vender bitcoin, pero también conlleva importantes compensaciones. Los intercambios centralizados son empresas que permiten a los clientes comprar y vender bitcoin directamente a través de ellos. Sin embargo, esta comodidad tiene un costo.



Centralizados

Intercambios centralizados y sus compensaciones

Es importante señalar que al comprar Bitcoin a través de un intercambio centralizado, a menudo se requiere proporcionar información personal y verificar tu identidad. Esto crea un riesgo de robo de identidad y expone tu información personal a posibles amenazas. Además, los intercambios centralizados retienen tus bitcoins, lo que significa que no tienes control sobre tu dinero hasta que lo retiras de ellos.

Para aumentar las preocupaciones, los intercambios centralizados pueden malversar los fondos de los usuarios o prestar más bitcoins de los que tienen en reservas hasta que colapsan. ¡Sí, al igual que los bancos! Sin embargo, en el mundo Bitcoin, no hay un banco central que rescate a los bancos fraudulentos imprimiendo más moneda, porque no se puede "imprimir" más bitcoin.

Cómo Utilizar Bitcoin

7.2 Introducción a los Monederos de Bitcoin

A diferencia del dinero físico, los bitcoins no están realmente presentes en un monedero de Bitcoin. Viven en el libro mayor distribuido que la red de Bitcoin verifica y asegura constantemente. Entonces, ¿cómo puedes ser dueño de bitcoin?

Tienes propiedad de tus bitcoins solo cuando posees las claves privadas que te permiten firmar transacciones y transferir la propiedad de tus bitcoins de ti a otra persona. Este es el acto de enviar bitcoins. Con eso en mente, echemos un vistazo a dos conceptos que describimos al usar el término "monedero":



- ◆ Una clave privada maestra (que es como una contraseña) a partir de la cual puedes generar claves públicas que puedes compartir con otros para recibir y enviar bitcoins.
- ◆ La interfaz móvil o de escritorio desde la cual puedes interactuar con la red de Bitcoin para consultar tu saldo de bitcoins, enviar y recibir transacciones y difundirlas a la red. Diferentes tipos de monederos, junto con sus beneficios y compensaciones, se describirán en la próxima sección.

7.2.1 Monederos Auto Custodios vs. Monederos Custodiados

Antes de detallar los diferentes tipos de monederos de Bitcoin y sus características, hagamos una importante distinción entre los monederos autogestionados y los custodiados, como se muestra en la tabla a continuación. Puedes observar los beneficios y riesgos de usar cada tipo de monedero y quién controla los bitcoins en cada caso. Autocustodia significa que el usuario posee las claves privadas, lo que implica que tienen verdadera posesión de sus bitcoins, mientras que en el segundo tipo, un tercero es quien custodia sus bitcoins.

Tipo de monedero	¿Quién controla mis bitcoins?	Beneficios	Riesgos
Billetera de Autocustodia	El usuario	Completo control sobre los fondos y transacciones sin proceso de aprobación ni congelación de cuentas, sin control corporativo o gubernamental. Protegido contra confiscaciones arbitrarias, como guardar el dinero en casa	No hay recuperación si se pierde la frase de recuperación, menos atención al cliente, la responsabilidad total recae en el usuario.
Billetera custodia	El proveedor externo	Fácil recuperación si se pierde el acceso, atención al cliente más fácil	Los fondos siempre están conectados a Internet, por lo que son más vulnerables a hackeos y brechas de seguridad. Los custodios controlan y pueden congelar cuentas.

Capítulo #7

En un monedero de auto custodia (también llamado monedero no-custodio), eres el único con las claves del monedero y tienes control total sobre lo que entra y sale. Por otro lado, en un monedero custodio, otra persona posee la clave y puede acceder y gestionar el contenido del monedero en tu nombre.

- 💡 La auto custodia es como ser tu propio banco. Las transacciones no están sujetas al control o autoridad de ningún gobierno o empresa, pero también significa que llevas la completa responsabilidad de mantener seguros tus bitcoins.
- 💡 La auto custodia asegura que terceros no puedan confiscar tus bitcoins sin tu consentimiento.
- 💡 La auto custodia brinda tranquilidad en tiempos de incertidumbre, sabiendo que tus bitcoins están seguros.

Es importante elegir el tipo correcto de monedero según las necesidades individuales. A veces, a las personas les resulta difícil distinguir si están instalando un monedero auto custodio o un monedero custodio. Esta tabla muestra las diferencias en el proceso de instalación.

Tipo de monedero	Paso 1: Elige un monedero	Paso 2: Instala el monedero	Paso 3: Crea un nuevo monedero	Paso 4: Asegura tu frase semilla	Paso 5: Comienza a usar tu monedero
Monedero de Autocustodia	Elige un proveedor de monedero de autocustodia	Sigue las instrucciones del proveedor	Genera la frase de recuperación y al menos una llave privada	Guarda la frase de recuperación en un lugar seguro	Comienza a usar tu monedero para recibir y enviar bitcoin
Monedero de Custodia	Elige un proveedor de monedero custodio	Sigue las instrucciones del proveedor	Crea una cuenta con el proveedor del monedero	N/A (el proveedor es el que tiene la llave privada)	Comienza a usar tu monedero para recibir y enviar bitcoin



**Sin tus claves
no son tus monedas**

"Sin tus claves, no son tus monedas" es un dicho popular entre los poseedores de bitcoins. Se refiere a la idea de que si no tienes control directo sobre las claves privadas asociadas con tu monedero de bitcoin, no tienes verdadera propiedad de las monedas.

Quien quiera que acceda a tus claves privadas obtendrá la propiedad de tus bitcoins. Por eso es de suma importancia protegerlas manteniéndolas lejos de miradas indiscretas. Veremos algunas formas de hacerlo más adelante en el libro. Para lo que sigue, estaremos hablando solo de monederos auto custodios, donde el usuario posee sus propias claves y tiene control completo sobre sus bitcoins.

No te preocupes si se complica o no entiendes todo. Esto es un viaje y comprenderás más a medida que empieces a usar Bitcoin más.

Cómo Utilizar Bitcoin

7.2.2 Diferentes tipos de monederos de Bitcoin

Según dónde se creen y almacenen tus claves privadas, comúnmente utilizamos nombres diferentes para describir los monederos de Bitcoin. Si las claves se almacenan en tu teléfono inteligente, podemos llamarlo "monedero móvil". Si se almacenan de forma segura en un dispositivo dedicado, lo llamaremos "monedero de hardware". Si la clave se almacena solo en papel, entonces se puede llamar "monedero de papel".

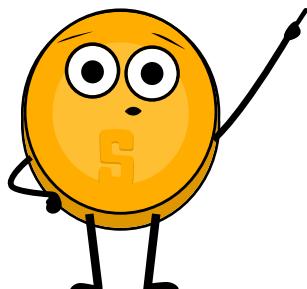
Aquí tienes una tabla que presenta los diferentes nombres que damos a los monederos de Bitcoin, según la estructura que tengan:

Tipo de monedero	Descripción	Ventajas	Desventajas	Ejemplo de uso
Monedero Online	Un monedero al que se accede a través de un navegador web	Accesible desde cualquier dispositivo con conexión a internet. Fácil de usar.	Menos seguro. Puede ser hackeado o comprometido	Alguien que necesita acceder a su monedero frecuentemente y no tiene muchos fondos que guardar
Monedero Móvil	Monedero que se puede instalar en un celular móvil	Conveniente. Se puede accesar desde adonde sea	Se puede perder si el dispositivo/celular se pierde o es robado o hackeado	Alguien que necesita hacer transacciones sobre la marcha y no tiene muchos fondos para almacenar.
Monedero de escritorio	Monedero que se instala en una computadora de escritorio	Más seguro que monederos en línea. Pueden usarse sin conexión	Pueden ser hackeados si la computadora es infectada con malware	Alguien que quiera almacenar una gran cantidad de bitcoins y se sienta cómodo usando una computadora de escritorio.
Monedero Hardware	Un dispositivo físico que almacena bitcoins sin conexión.	Muy seguros. Pueden usarse sin conexión	Los fondos podrían ser irrecuperables si el dispositivo se pierde o es robado	Alguien que quiera almacenar un gran cantidad de bitcoins y está dispuesto a pagar por la seguridad adicional de un monedero o billetera hardware.
Monedero de papel	Un registro físico de las claves públicas y privadas de una billetera Bitcoin.	Muy seguros. Pueden usarse sin conexión	Puede perderse o ser robados si el registro físico se pierde o es robado.	Alguien que quiera almacenar una gran cantidad de bitcoins y esté dispuesto a tomar precauciones adicionales para garantizar su seguridad.



Capítulo #7

Dado que las claves pueden moverse de un dispositivo a otro, el "estado" de tu monedero de Bitcoin no es definitivo. Por ejemplo, si genero las claves de mi monedero de Bitcoin en una computadora y luego las cargo en mi teléfono, el "monedero de escritorio" se convierte en un "monedero móvil".



Cuando se trata de almacenar tus bitcoins, no solo se trata de quién tiene control sobre ellos, sino que también hay muchos otros riesgos a considerar. Por eso es importante encontrar una solución de almacenamiento que sea segura y conveniente.

Cuando analizas las compensaciones de los diferentes tipos de monederos, aprenderás que no hay un monedero ideal que satisfaga todas las necesidades.

Al elegir un monedero de Bitcoin, hay varias cosas que debes considerar:

- 💡 **Seguridad:** Asegúrate de que el monedero tenga fuertes medidas de seguridad, como autenticación de dos factores y políticas de contraseñas seguras.
- 💡 **Privacidad:** Considera si el monedero te permite permanecer anónimo o si requiere información personal para configurar una cuenta.
- 💡 **Facilidad de uso:** Elige un monedero que sea fácil de usar y navegar, especialmente si eres nuevo en Bitcoin.
- 💡 **Compatibilidad:** Asegúrate de que el monedero sea compatible con tu dispositivo y sistema operativo.
- 💡 **Tarifas:** Compara las tarifas cobradas por diferentes monederos para asegurarte de obtener la mejor oferta.
- 💡 **Reputación:** Investiga la reputación del monedero y su equipo para asegurarte de que sea de confianza.
- 💡 **Control:** Algunos monederos te dan más control sobre tus claves privadas, lo que puede ser una ventaja de seguridad.

Considera si quieres un monedero que te dé control total o uno que sea más fácil de usar pero que pueda tener menos control.

7.2.3 Código abierto vs. código cerrado

Otro factor importante a tener en cuenta al elegir un monedero de Bitcoin es saber si la aplicación o el software es de código abierto o no.

El código abierto es muy importante porque permite a la comunidad revisar el código y continuar desarrollando el proyecto si el equipo dejara de trabajar en él.

Cómo Utilizar Bitcoin



Así como el código de Bitcoin está completamente abierto para que todos lo revisen, usen y modifiquen, también debería ser el código del monedero que uses para almacenar tus bitcoins.

Actividad - Discusión en clase y evaluación de monederos de Bitcoin en bitcoin.org

Ve al siguiente sitio web:

<https://bitcoin.org/es/elige-tu-monedero> y utiliza tu nuevo conocimiento sobre monederos de Bitcoin para seleccionar el mejor según los criterios que discutimos hoy.



7.3 Configuración de un monedero de Bitcoin móvil

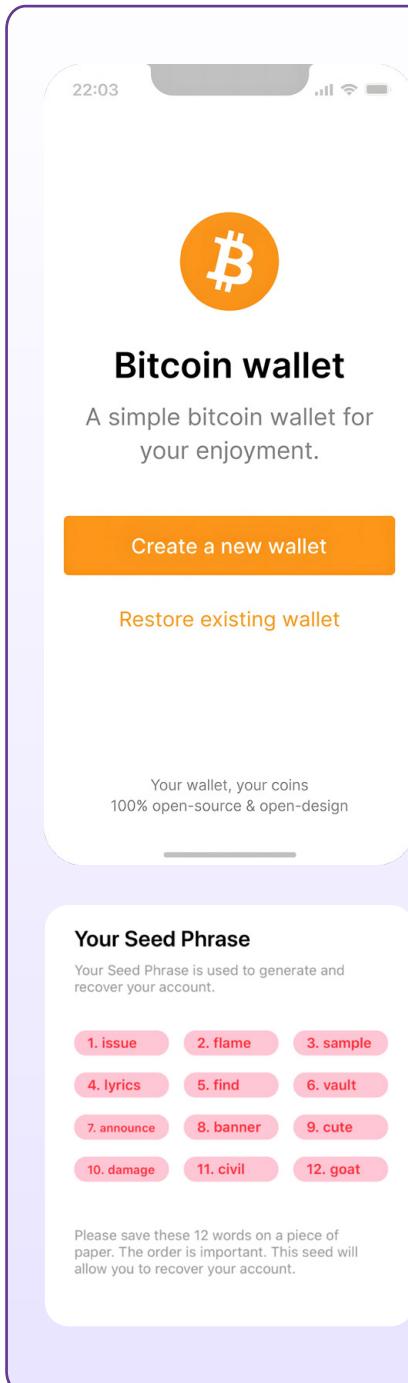
Ahora que tenemos una mejor comprensión de los monederos de Bitcoin y sus diferencias, veremos cómo usar uno en la práctica. Para este ejemplo, crearemos un monedero móvil directamente en nuestro teléfono inteligente.

Actividad: Crear tu primer monedero de Bitcoin

Si los estudiantes no tienen teléfonos celulares, el profesor proporcionará uno a los estudiantes para que lo tomen prestado.

Hay dos opciones para esta actividad:

Capítulo #7



The smartphone screen displays a mobile application for managing a Bitcoin wallet. At the top, there is a status bar showing the time (22:03) and signal strength. Below the status bar, the app's interface includes:

- A large orange circular icon containing a white Bitcoin symbol.
- The text "Bitcoin wallet" in bold.
- A subtitle: "A simple bitcoin wallet for your enjoyment."
- An orange button labeled "Create a new wallet".
- A smaller orange button labeled "Restore existing wallet".
- A text box stating: "Your wallet, your coins" and "100% open-source & open-design".
- A section titled "Your Seed Phrase" with the sub-instruction: "Your Seed Phrase is used to generate and recover your account." It lists 12 words in three rows of four: 1. issue, 2. flame, 3. sample; 4. lyrics, 5. find, 6. vault; 7. announce, 8. banner, 9. cute; 10. damage, 11. civil, 12. goat.
- A note at the bottom: "Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account."

**Ejercicio en clase:
Opción 1 — Descargar un nuevo monedero.**

Cómo crear y usar un monedero de Bitcoin:

- 1 Busca la aplicación en la App Store (iOS) o en Google Play Store (Android).
- 2 Abre la aplicación e ingresa tu frase de recuperación de 12 o 24 palabras (a veces llamada frase semilla). ¡Asegúrate de anotarla y guardarla en un lugar seguro! Esta frase de recuperación te permite recuperar el acceso completo a tus fondos si es necesario.

Recuerda que si pierdes u olvidas esta secuencia de palabras, no podrás acceder a tus bitcoins si pierdes el acceso a tu monedero.

- 3 Debes confirmar que realmente has guardado tu frase de recuperación o frase semilla. Para hacer esto, debes ingresar, en el mismo orden, las palabras de tu frase semilla.
- 4 Como medida adicional de seguridad, algunos monederos permiten elegir una contraseña segura. Tu clave privada y la primera dirección de bitcoin se crean automáticamente para ti por tu monedero.

Piensa en tu dirección pública como tu dirección de correo electrónico, quieres compartirla con otros para que te envíen bitcoins, o en el caso de una dirección de correo electrónico, un correo electrónico.

Piensa en tu dirección privada como la contraseña de tu correo electrónico, no querrías compartirla con nadie, ya que les daría acceso a tu correo electrónico.

- 5 Utiliza tu dirección de "recibir" para recibir bitcoins. Transfiere bitcoins a tu monedero. Con un monedero auto custodio, no siempre puedes comprar bitcoins directamente con moneda fiduciaria, así que es posible que necesites comprar y transferirlos desde un intercambio primero.

Cómo Utilizar Bitcoin

22:03

Back

This is your recovery phrase
Make sure to write it down as shown here. You have to verify this later.

1	gloom	2	police
3	month	4	stamp
5	viable	6	claim
7	hospital	8	heart
9	alcohol	10	off
11	ocean	12	ghost

Backup to iCloud

Print template

Verify

**Ejercicio en clase:
Opción 2 — Restaurar monedero (Con límite de tiempo)**

Descarga un monedero de bitcoin y agrega algunos satoshis para cada estudiante.

Dale a cada estudiante una hoja con una frase semilla para recuperar un monedero.

Guía a los estudiantes paso a paso:

- 1 Cuando inicias tu monedero por primera vez, verás tres métodos de creación de monedero, toca [Importar un monedero existente]. Verás una pantalla de introducción, toca [Restaurar con frase de recuperación].
- 2 Ingresa tu frase de recuperación de 12,18 o 24 palabras una por una, en el orden correcto.
- 3 Toca [Restaurar/Restaurar] cuando hayas terminado.
- 4 Verás un modo "Importación exitosa" cuando tu monedero se haya importado correctamente.

7.4 Recepción y envío de transacciones

Una transacción de bitcoin es una transferencia de propiedad de bitcoins existentes a un nuevo propietario. Pero en lugar de transferir monedas físicas, todos los nodos en la red actualizan su copia local del libro público para reflejar el cambio de propiedad.

Al enviar una transacción de Bitcoin, el remitente firma un mensaje que solo él puede firmar con su clave privada, indicando a la red que la propiedad de los bitcoins cambia a la dirección del destinatario.

Los bitcoins ahora estarán vinculados a una dirección desde la cual solo el nuevo propietario puede enviar, dándole la propiedad de los bitcoins.

Libro contable

Propietario de la cuenta	Saldo
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniel	5.25

Mensaje de solicitud de transacción de Bitcoin
Jim envía 0.50 BTC a Eliana
Jim ➔ Eliana 0.50 BTC

Libro contable

Propietario de la cuenta	Saldo
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.00
Robert	2.00
Eliana	2.25
Daniel	5.25

Las nuevas transacciones de Bitcoin se inicien desde monederos de todo el mundo, pero no hay un procesador de pagos central. En cambio, los mineros de todo el mundo compiten para registrar las transacciones en el libro contable.

Digamos que Jim le debe 0.5 BTC a Eliana y está listo para pagarle. Ambos tienen monederos digitales.



- 1 Eliana comparte su dirección con Jim.
- 2 Jim utiliza su software de monedero para crear la transacción, que incluye la dirección de Eliana, la cantidad a transferir (0.5 BTC) y una tarifa para el minero.
- 3 Despues de firmar la transacción, se transmite a la red, donde es verificada por nodos. Los nodos verifican la transacción para validarla y asegurarse de que Jim tenga fondos suficientes. Si no los tiene, rechazan la transacción de inmediato.
- 4 Una vez que la transacción es verificada, los mineros la añaden al blockchain, y los fondos se transfieren a la dirección de Eliana.
- 5 Luego, Eliana puede usar su clave privada para acceder a los fondos transferidos en su monedero.

Es importante destacar que una vez que la transacción está completa, no se puede revertir.

Cómo funciona una transacción de Bitcoin



Recepción de transacciones de bitcoin:



Para recibir bitcoin, deberás proporcionar al remitente la dirección de tu monedero de bitcoin. Esta es una cadena única de letras y números que representa tu monedero y se utiliza para identificarlo en la red de Bitcoin. Puedes encontrar tu dirección de monedero al iniciar sesión en tu monedero de Bitcoin y buscar la opción de "Recibir" o "Depositar" bitcoins.

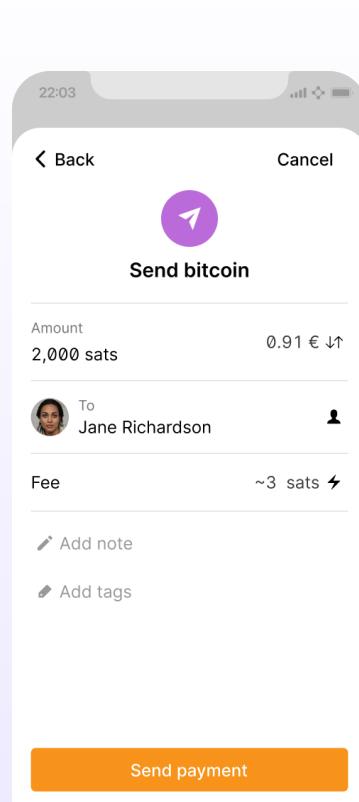
Luego, puedes compartir tu dirección de bitcoin con el remitente de varias maneras:

- 1 Copiar y pegar la dirección: Puedes copiar la dirección seleccionándola y presionando "Copiar" en tu teclado, luego pegarla en un correo electrónico o mensaje al remitente.
- 2 Compartir un enlace a tu monedero de Bitcoin: Algunos monederos de Bitcoin permiten crear un enlace a tu monedero que puedes compartir con el remitente. Luego pueden hacer clic en el enlace para acceder a tu monedero y enviar los bitcoins.
- 3 Compartir un código QR: Si el remitente tiene un teléfono inteligente con una aplicación de monedero de Bitcoin, pueden escanear el código QR para obtener tu dirección de bitcoin.

Cómo Utilizar Bitcoin

Una vez que el remitente tiene tu dirección de bitcoin, pueden enviarte los bitcoins ingresando tu dirección y la cantidad que desea enviarte e iniciando la transacción. Los bitcoins luego se enviarán a tu monedero y serán visibles una vez que la transacción se confirme en la red de Bitcoin. Esto suele tomar unos minutos.

A continuación, veremos cómo realizar transacciones de envío de bitcoin.



Envío de transacciones de bitcoin:

Para enviar bitcoins, necesitarás algunas cosas: un monedero de Bitcoin, la dirección de bitcoin del destinatario y la cantidad de bitcoins que deseas enviar.

- 1 Abre tu monedero de Bitcoin. Se enviará un código SMS a tu número de teléfono, y deberás ingresararlo en el cuadro de diálogo. Alternativamente, si has habilitado la autenticación de dos factores de Google, deberás ingresar el código de seis dígitos de la aplicación Google Authenticator.
- 2 Ve a la función "Enviar" o "Retirar" y copia la dirección del destinatario.
- 3 Ingresa la dirección de bitcoin del destinatario pegándola en el campo "Para".
- 4 Ingresa la cantidad de bitcoins que deseas enviar en el campo "Cantidad".
- 5 Verifica la dirección del destinatario y la cantidad a enviar.
- 6 Antes de hacer clic en Confirmar y Enviar, te recomendamos que verifiques los detalles de la transacción una vez más para asegurarte de que estás enviando la cantidad correcta de bitcoins a la dirección de monedero correcta.
- 7 Confirma la transacción y espera a que la red confirme la transacción.

Ahora sabes cómo evaluar, seleccionar y configurar un monedero de Bitcoin auto custodio. Enviar bitcoins de un monedero a otro en la red de Bitcoin se llama enviar una transacción "en cadena". Esto se debe a que la transacción ocurre en la cadena de bloques principal de la red Bitcoin. Las transacciones en cadena son la forma más segura de realizar transacciones con bitcoins; sin embargo, son más costosas y lentas que otras opciones que discutiremos en el Capítulo 8.

Actividad: Transacciones de Bitcoin en Acción

Objetivo: Comprender los conceptos y mecanismos subyacentes de una transacción de Bitcoin peer-to-peer.

Antes de comenzar, aquí hay un recordatorio rápido sobre los actores clave en una transacción de Bitcoin:

- Los Remitentes y Receptores son las partes que desean realizar una transacción entre ellas.
- Los Nodos validan las transacciones y almacenan una copia completa del blockchain. *Los nodos ligeros permiten a las personas validar transacciones utilizando menos almacenamiento y menos recursos computacionales.
- Los Mineros son responsables de agregar nuevas transacciones a la blockchain.



Comprende tu papel. Se te ha asignado uno de los siguientes roles: remitente, receptor, nodo o minero.

- 💡 Los Remitentes serán responsables de crear y transmitir transacciones.
- 💡 Los Receptores serán responsables de recibir y verificar transacciones.
- 💡 Los Nodos serán responsables de validar las transacciones al verificar que la transacción sea válida.
- 💡 Los Mineros serán responsables de agregar las transacciones al blockchain.

Tanto los nodos como los receptores deben verificar las transacciones:

1 Como remitente: Crea una transacción.

Para crear una transacción, sigue estos pasos: Toma una nota de transacción y escribe la cantidad de monedas que deseas enviar y el nombre o iniciales del receptor. Firma la nota con tu nombre o iniciales, simulando una clave privada. Pasa la nota de transacción y la cantidad correspondiente de monedas al receptor.

2 Como receptor: Eres responsable de verificar las transacciones. Sigue estos pasos:

- 💡 Verifica la nota de transacción para asegurarte de que se haya escrito la cantidad correcta de monedas y el nombre o iniciales del receptor.
- 💡 Cuenta las monedas recibidas y compáralas con la cantidad de monedas escrita en la nota.
- 💡 Si las monedas coinciden, marca la casilla de aprobación. Si las monedas no coinciden o tienes dudas, rechaza la transacción.

Moneda enviada	Remitente	Firma del remitente	Receptor	Fecha y hora	Aprobación del destinatario

3 Como nodo: Verifica y valida transacciones. Eres responsable de verificar que la transacción sea válida

- 💡 Verifica que la dirección del remitente sea válida y que la dirección del receptor sea válida.
- 💡 Asegúrate de que el remitente tenga fondos suficientes para completar la transacción y de que la transacción no duplique el gasto de ninguna moneda.

Moneda enviada	Remitente	Firma del remitente	Receptor	Fecha y hora	Aprobación del nodo

Cómo Utilizar Bitcoin

4 Como minero: agrega transacciones al blockchain. Eres responsable de agregar las transacciones al blockchain. Sigue estos pasos:

- ✿ Verifica las transacciones aprobadas por los receptores y validadas por los nodos.
- ✿ Lanza los datos y compara los números con otro minero. El minero con el número más pequeño agregará la transacción al blockchain.
- ✿ Por tu tiempo, energía y esfuerzo, ganarás un punto. Al final de la actividad, el minero con más puntos gana.

**Una vez que una transacción se agrega al blockchain, no se puede cambiar ni revertir.

5 Lleva un registro de tu saldo de monedas: A lo largo de la actividad, lleva un registro de tu saldo de monedas contando las monedas en tu monedero digital.

Moneda enviada	Remitente	Firma del remitente	Receptor	Fecha y hora	Aprobación

6 Discute los conceptos aprendidos con tu clase.

7.5 Ahorro en bitcoin

Bitcoin es una forma de resguardar tu dinero contra la inflación y protegerlo de ser controlado por cualquier otra persona, si lo haces correctamente. Ahorrar en bitcoin proporciona un vehículo para almacenar, acumular y construir riqueza con el tiempo. Como ya comprendes, el tipo de dinero que elijas para ahorrar es una de las decisiones más importantes que puedes tomar. Elegir sabiamente te permite construir un futuro mejor para ti y tu familia.

Paz mental: Cuando se almacena correctamente, Bitcoin es la única forma de propiedad que nadie puede quitarte.



7.6 No confíes, verifica

Lo que sea que hagas en Bitcoin, recuerda esto: "No confíes, verifica". No hay líderes en Bitcoin. Nunca deberías seguir ciegamente las afirmaciones de alguien. Además, siempre debes cuestionar lo que te dicen y verificarlo por ti mismo. Siguiendo este mantra, te protegerás de perder tus bitcoins. Esto se aplica tanto a afirmaciones como "el próximo Bitcoin" como a "oportunidades de inversión" o promesas de "ganancias rápidas y fáciles".

En resumen, el Capítulo 7 te ha proporcionado las habilidades importantes para usar Bitcoin en tu vida cotidiana. Aprendiste cómo obtener y intercambiar bitcoins de diferentes maneras y cómo mantenerlo seguro utilizando diversos monederos.

Al configurar tu monedero móvil de Bitcoin y realizar transacciones con otras personas, ahora tienes experiencia práctica para usar bitcoin con confianza en tu día a día. Comprendiendo Bitcoin como una forma de ahorrar dinero y siguiendo la idea de "No confíes, verifica", ahora tienes el control de tu dinero.

En el próximo capítulo, exploraremos la red lightning. Veremos cómo esta tecnología innovadora está cambiando la forma en que las personas en todo el mundo acceden y utilizan el dinero. Desde transacciones cotidianas hasta aplicaciones más avanzadas, aprenderás cómo la red lightning capacita a individuos, comunidades y empresas al proporcionarles acceso a servicios financieros.

Capítulo #8

Red lightning: Utilizando Bitcoin en tu Vida Diaria

8.0 Introducción

Actividad - Ver "Bitcoin Lightning Network Explicado: Cómo Funciona en Realidad"

8.1 La red Lightning

8.2 Diferentes tipos de Billeteras Lightning

8.2.1 Billeteras de autocustodia vs. Billeteras de custodia

8.2.2 Código abierto vs. Código cerrado

8.3 Configuración de una Billetera Bitcoin Lightning

8.4 Envío y recepción de Transacciones Lightning

Actividad: Carrera de relevos con Billeteras Lightning **8.5**

Comprar Café y Comestibles con Bitcoin

8.5.1 En línea: Plugins de pago — Comercio electrónico

8.5.2 En persona: Encontrar un comerciante en tu área

8.5.3 Herramientas de transición: Tarjetas de regalo y

Tarjetas de pago

8.5.4 Economías Circulares y Bitcoin como Medio de Intercambio

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

Red Lightning: Utilizando Bitcoin en tu Vida Diaria

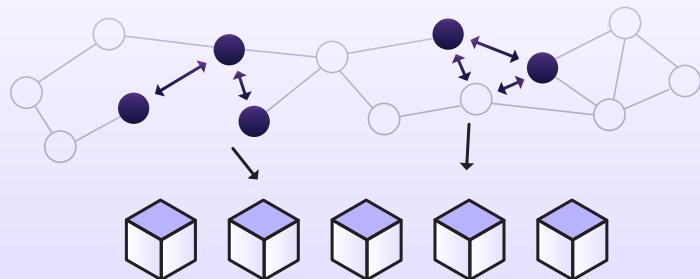
8.0 Introduction

“Estamos construyendo la red Visa para Bitcoin. Pero lo que creo que es poderoso, a diferencia de Visa, cualquiera puede construir encima de ella.”

Elizabeth Stark

Las tecnologías suelen crecer y expandirse en capas, como una pila. Piensa en tu sitio web favorito, correo electrónico o redes sociales: se construyeron sobre el protocolo de Internet, que se construyó sobre computadoras, que se construyeron sobre electricidad, etc. Estas tecnologías comenzaron con un diseño muy simple y continuaron mejorando con el tiempo.

Bitcoin no es una excepción. Como dijo famosamente Andreas Antonopoulos: Bitcoin es el Internet del Dinero. Es la capa base de un dinero digital sólido, proporcionando una base sólida sobre la cual se construirán nuevas tecnologías.

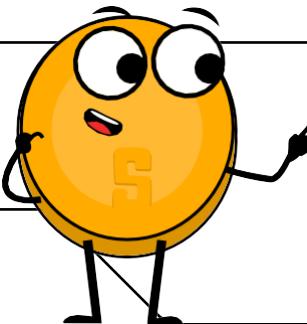


Una de estas capas se llama la Red Lightning. La Red Lightning es como una autopista súper rápida para Bitcoin. Ayuda a las personas a enviar y recibir bitcoin rápidamente y con tarifas muy bajas. Permite a los usuarios realizar transacciones instantáneas y pequeñas además de la red Bitcoin regular. ¡Esto facilita la compra de un café o el pago a un amigo de manera simple y rápida!

Recuerda: Un Satoshi es como la moneda más pequeña de Bitcoin. Al igual que un dólar se puede dividir en centavos, un Bitcoin se puede dividir en unidades más pequeñas llamadas Satoshis. Un Bitcoin equivale a 100 millones de Satoshis, haciendo que los Satoshis sean las partes más pequeñas de valor en el sistema Bitcoin. En este capítulo, cuando hablaremos de enviar bitcoin a través de la Red Lightning, lo llamaremos "enviar sats", que son simplemente partes más pequeñas de un Bitcoin.

Sats	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00010000
10,000	0.00100000
100,000	0.01000000
1,000,000	0.10000000
10,000,000	0.10000000
100,000,000	1.00000000

Actividad: Mira este video sobre la Red Lightning



8.1 La Red Lightning

Como acabamos de ver, la Red Lightning sirve como un sistema de pago que facilita transacciones rápidas y rentables con bitcoin. Funciona estableciendo una billetera compartida donde ambas partes tienen algo de bitcoin. Pueden realizar numerosas transacciones entre sí sin necesidad de registrar cada una en el libro mayor principal. El saldo final se registra en el libro mayor una vez que se completan las transacciones.



La red Lightning es un sistema de pago que permite a los usuarios enviar y recibir pagos de forma rápida y económica utilizando bitcoin. Funciona creando un monedero compartido en el que ambas personas almacenan sus bitcoins y luego realizan transacciones ilimitadas entre sí sin tocar la blockchain principal. Cuando terminan, el saldo final se registra en la blockchain principal.

Imagina un día en el que te vas a trabajar a una cafetería. Anticipando una estadía de todo el día, abres una cuenta y prepagas algo de dinero en lugar de pagar cada vez que ordenas algo. Cuando estás listo para irte al final del día, tú y el dueño revisan la cuenta para liquidar la factura final. Si pagaste más de tu consumo real, recibes algo de dinero de vuelta.

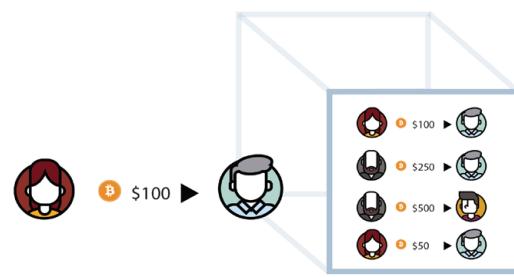
Ahora, imagina a miles de personas haciendo lo mismo simultáneamente y permitiendo que otros utilicen sus cuentas para conectarse con más personas. ¡Esa es la Red Lightning!

Con Lightning, puedes hacer pagos a cualquier persona en la red, no solo a la persona con la que comparten una cuenta directa. Tu pago puede navegar a través de la red hasta que llegue a su destino, incluso si no tienes un canal abierto con el destinatario.

Echemos un vistazo a la diferencia entre las transacciones en cadena (el tipo que discutimos en el Capítulo 7) y las transacciones fuera de cadena (Red Lightning):

Transacciones en cadena:

Estas son transacciones que ocurren directamente en la cadena de bloques de Bitcoin. Tardan unos 10 minutos en confirmarse y las tarifas dependen del tamaño de la transacción en bytes. Son más seguras pero más lentas.

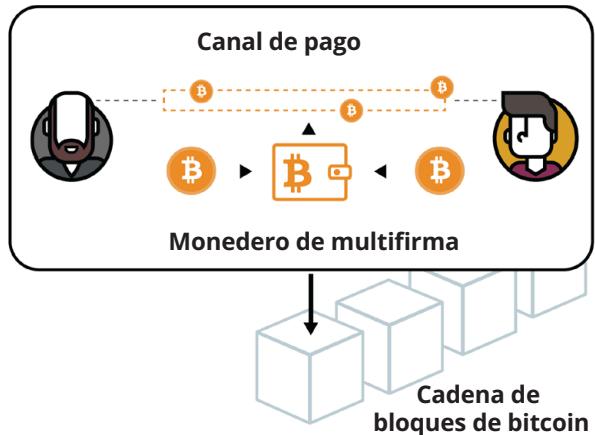


Red Lightning: Utilizando Bitcoin en tu Vida Diaria

Transacciones fuera de cadena (Red Lightning)

Estas transacciones ocurren en una red separada construida sobre la cadena de bloques de Bitcoin. Se liquidan más rápido y con tarifas más bajas.

Se utilizan comúnmente donde las regulaciones y leyes respaldan su adopción y donde características como la velocidad y el costo de las transacciones son más importantes. En comparación con las transacciones en cadena, son menos seguras.



Red de Pago	Red Bitcoin	Red Lightning
Definición	Una red digital descentralizada que utiliza criptografía para proteger las transacciones financieras.	Un protocolo de pago de segunda capa que opera sobre la cadena de bloques de Bitcoin, lo que permite transacciones más rápidas y económicas.
Ventajas	Descentralizado y seguro. Sin devoluciones de cargo ni fraude. Se puede utilizar de forma anónima. Aceptación mundial	Transacciones más rápidas y baratas. Mayor escalabilidad. Las transacciones fuera de la cadena no obstruyen la cadena de bloques.
Desventajas	Tiempos de transacción lentos. Tarifas elevadas para ciertos tipos de transacciones. Complejo para principiantes.	Requiere confianza en los operadores del canal. Todavía experimental y no ampliamente adoptado. Requiere transacciones en cadena para abrir y cerrar canales.



Capítulo #8

8.2 Diferentes tipos de Billeteras Lightning

Una billetera Lightning es un poco diferente a una billetera de Bitcoin, aunque realiza la misma función: recibir y enviar bitcoin. La diferencia es que una billetera Lightning te permite enviar bitcoin en la red Lightning, que es una segunda capa sobre la red Bitcoin.

Al igual que vimos en el capítulo anterior con las billeteras de Bitcoin, las billeteras Lightning tienen diferentes características que deben considerarse antes de elegir una.

8.2.1 Billeteras Autocustodias vs. Billeteras Custodias

Las billeteras Lightning se pueden dividir en categorías muy específicas, pero por simplificación, las dividiremos en dos: billeteras autocustodias y billeteras custodias.

Al igual que las billeteras de Bitcoin, una billetera Lightning autocustodia es aquella en la que controlas las claves de la billetera, mientras que una billetera Lightning custodia es aquella en la que otra persona controla las claves.

Al usar una billetera custodia, solo se te da acceso a la billetera, pero dependes de otra persona para obtener permiso para usar tu dinero. Estás renunciando a la propiedad de tu dinero por conveniencia.

Esto puede ser aceptable para cantidades pequeñas, aunque se recomienda usar una billetera autocustodia una vez que entiendas la tecnología.

Para lo que sigue, solo hablaremos de billeteras Lightning autocustodias.

8.2.2 Código abierto vs. Código cerrado

Al igual que las billeteras de Bitcoin que vimos en el capítulo anterior, las billeteras Lightning pueden ser de código abierto o de código cerrado. Siempre utiliza billeteras de código abierto, ya que están completamente abiertas para su revisión y evaluadas por la comunidad.

Una aplicación de código abierto también significa que cualquiera puede contribuir a la mejora del software, haciéndola una mejor elección para los usuarios.

8.3 Configuración de una Billetera Bitcoin Lightning

Configurar una billetera Bitcoin Lightning autocustodia es igual que configurar una billetera Bitcoin en cadena autocustodia.

Red Lightning: Utilizando Bitcoin en tu Vida Diaria

Ejercicio de Clase. Opción 1. Descargar una nueva billetera Lightning autocustodia

Cómo crear y usar una billetera Bitcoin Lightning:

- 1** Busca la aplicación en la App Store (iOS) o Google Play Store (Android)
- 2** Abre la aplicación e ingresa tu frase de recuperación de 12 o 24 palabras (a veces llamada frase de semilla). ¡Asegúrate de anotarla y guárdala en un lugar seguro! Esta frase de recuperación te permite recuperar el acceso completo a tus fondos si es necesario.

Recuerda que si pierdes u olvidas esta secuencia de palabras, no podrás acceder a tu bitcoin si pierdes el acceso a tu billetera.

- 3** Debes confirmar que realmente has guardado tu frase de recuperación o semilla. Para hacer esto, debes ingresar, en el mismo orden, las palabras de tu frase de semilla.
- 4** Como medida adicional de seguridad, algunas billeteras te permiten elegir una contraseña segura. Tu clave privada y tu primera dirección de bitcoin se crean automáticamente para ti por tu billetera.
- 5** Genera una factura Lightning, una dirección o un código QR para recibir bitcoin. Transfiere bitcoin a tu billetera. Con una billetera autocustodia, no siempre puedes comprar bitcoin directamente con fiat, así que es posible que necesites comprarlo y transferirlo desde un intercambio primero.

Tu frase semilla

Su frase semilla se utiliza para generar y recuperar su cuenta.

- | | | | | |
|-----------------|-------------------|-----------------|-----------------|------------------|
| 1 Issue | 2 Flame | 3 Sample | 4 Lyrics | 5 Find |
| 6 Vault | 7 Scissors | 8 Banner | 9 Cute | 10 Damage |
| 11 Civil | 12 Goat | | | |

Por favor, guarda estas 12 palabras en un papel. El orden es importante. Esta semilla le permitirá recuperar su cuenta.

*Nota: si estás utilizando una billetera custodia, no necesitarás seguir algunos de los pasos en la sección 8.3. Usar una billetera custodia conlleva riesgos, ya que no tendrás control sobre tu clave privada, lo que significa que no tendrás control sobre el dinero que guardas en tu billetera.

Ahora que hemos configurado nuestra billetera Bitcoin Lightning, veamos cómo recibir y enviar transacciones Lightning, y cómo son diferentes de las transacciones en cadena que enviamos en el Capítulo 7.



8.4 Recepción y Envío de Transacciones Lightning

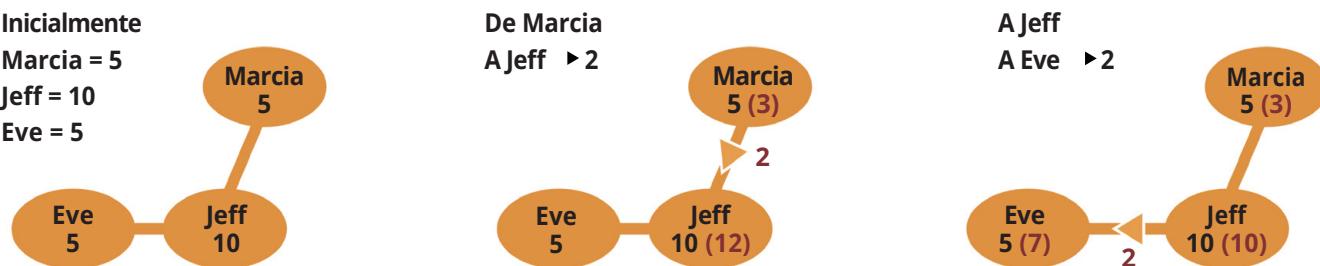
Con una Billetera Lightning, usar Bitcoin es rápido, barato y privado, facilitando las transacciones entre dos personas. Puedes enviar y recibir rápidamente Bitcoin para cosas cotidianas como comprar café o hacer compras.

Veamos algunos ejemplos de la Red Lightning en acción:

Ejemplo 1:

A continuación, Marcia tiene 5 unidades de alguna moneda y Eva tiene 5 unidades también. Marcia quiere enviar 2 de sus unidades a Eva, así que envía 2 unidades a Jeff. Jeff luego pasa las 2 unidades a Eva, quien ahora tiene 7 unidades. Marcia ahora tiene 3 unidades. ¡Y eso es todo! La transacción está hecha.

El punto clave aquí es que Marcia y Eva no tienen que pasar por un banco u otro intermediario para que ocurra la transacción.



Jeff actúa como intermediario o "tercero de confianza" en este escenario, donde Marcia y Eva no confían directamente entre sí. Jeff recibe las 2 unidades de Marcia y luego las pasa a Eva, completando así la transacción. Al utilizar a Jeff como intermediario, Marcia y Eva pueden completar la transacción sin necesidad de un banco u otra institución centralizada, lo que puede hacer que la transacción sea más rápida, más barata y más segura. Jeff es un elemento clave en este proceso de transacción peer-to-peer.

Como operador de nodo en una transacción de la Red Lightning, Jeff se beneficia de varias maneras:



Tarifas de transacción

Jeff gana una pequeña tarifa por cada transacción que pasa por su nodo, lo que lo compensa por el tiempo y el esfuerzo que invierte en mantener y ejecutar su nodo.



Participación en la red

Al ejecutar un nodo Lightning, Jeff está participando en la red y ayudando a aumentar su descentralización, seguridad y estabilidad. Esto puede aumentar la reputación y la credibilidad de Jeff como un operador de nodo confiable, haciéndolo un intermediario más atractivo para transacciones futuras.

Red Lightning: Utilizando Bitcoin en tu Vida Diaria

3

Crecimiento de la red

A medida que la Red Lightning crece y más personas la utilizan, es probable que aumente el número de transacciones que pasan por el nodo de Jeff, lo que puede resultar en un aumento de ingresos por tarifas de transacción.

4

Aumento de la seguridad de la red

El papel de Jeff como intermediario ayuda a aumentar la seguridad de la red al agregar una capa adicional de protección entre Marcia y Eva. Esto puede aumentar la confianza de los usuarios en la red, haciéndola más atractiva para nuevos usuarios y ayudando a impulsar el crecimiento. En resumen, ser un operador de nodo en la Red Lightning puede proporcionar a Jeff una fuente constante de ingresos, así como la oportunidad de contribuir al crecimiento y desarrollo de la red.

En resumen, las transacciones en cadena son más lentas pero más seguras, mientras que las transacciones fuera de cadena (Red Lightning) son más rápidas pero menos seguras. Debes considerar el equilibrio entre seguridad y velocidad según tus necesidades.

Ejemplo 2:

A Mirna le encanta McDonald's. ¡Va allí para desayunar, almorzar y cenar todos los días! Pero con tantas opciones de pago diferentes disponibles, no está segura de cuál es la mejor elección. Afortunadamente, ha aprendido un poco sobre Bitcoin y la Red Lightning. Después de comparar las tablas a continuación, Mirna no duda en usar un método de pago Lightning.

La Red Lightning frente al sistema bancario tradicional

Beneficios	Lightning	Sistema banca tradicional
Velocidad	Rápido	Lento
Transparencia	Transparente	Opaco
Seguridad	Seguro	Vulnerable
Tarifas de transacción	Bajo	Alto
Inclusión Financiera	Alto	Limitado

Beneficios	Lightning	Sistema banca tradicional
Escalabilidad	Alta	Baja
Privacidad	Alta	Moderada
Interoperabilidad	Alta	Baja
Cómplice legal	Moderada	Alta
Rentabilidad	Alta	Moderada

Visa, Inc.

En promedio 1,700 transacciones por segundo



Capacidad de 65,000 transacciones por segundo

Bitcoin On-chain



Capacidad de 7 transacciones por segundo

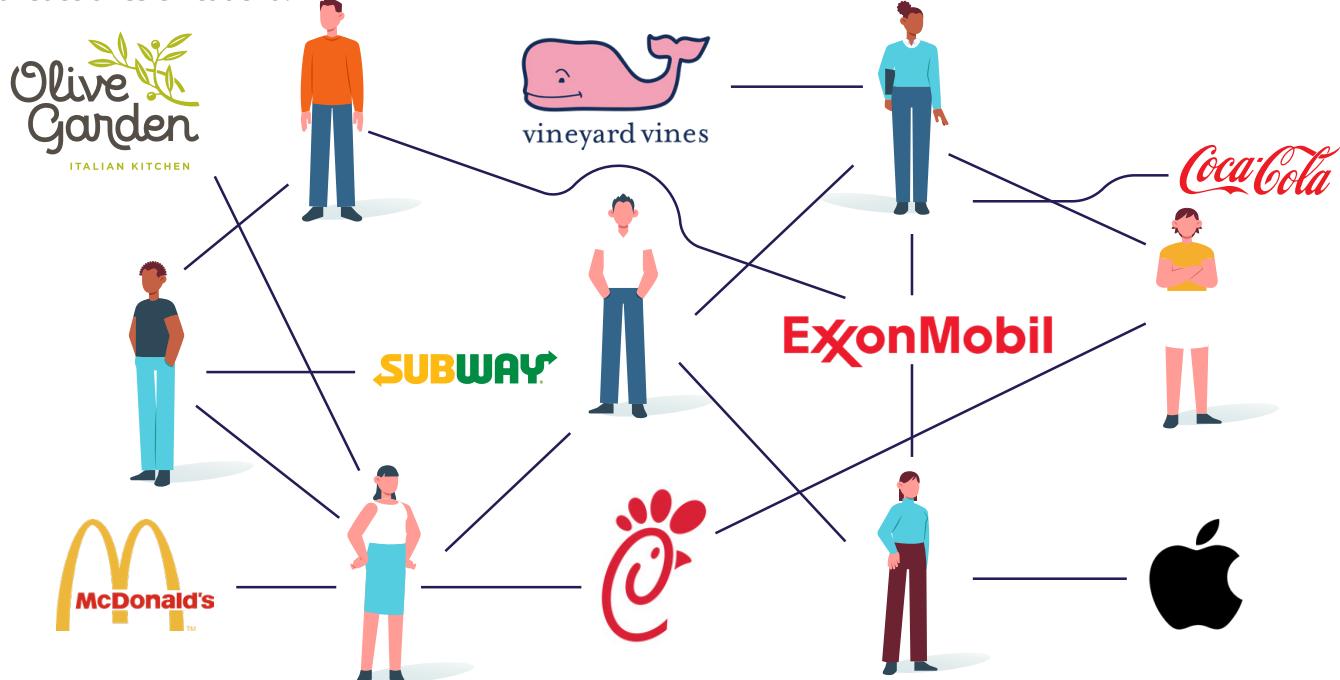
Bitcoin Lightning Network



Millones de transacciones por segundo

A Mirna también le gusta realizar transacciones rápidas, seguras y económicas, así que decidió usar Lightning para sus compras en McDonald's. Con Lightning, puede disfrutar aún más de sus comidas sabiendo que sus pagos se procesan al instante, de manera segura y con tarifas bajas. Además, dado que la Red Lightning proporciona inclusión financiera, Mirna ahora puede pagar sus comidas incluso si está en una zona remota en El Salvador.

Para comenzar con Lightning, Mirna descarga primero una Billetera Lightning en su teléfono. Luego, financia su Billetera Lightning enviando algo de bitcoin desde su billetera de bitcoin regular a su nueva Billetera Lightning. Este proceso se llama "financiar la billetera" o "financiar un canal de pago". Mirna puede financiar su billetera con la cantidad de bitcoin con la que se sienta cómoda, pero es importante tener en cuenta que la cantidad de bitcoin que bloquea en su Billetera Lightning no se puede usar en sus transacciones en cadena.



Una vez que su Billetera Lightning está financiada, puede usarla para hacer pagos en McDonald's.

McDonald's tiene un Nodo Lightning, por lo que Mirna puede abrir un canal de pago con ellos enviando algo de su bitcoin desde su Billetera Lightning a una dirección específica proporcionada por McDonald's. Esto mueve su bitcoin desde la cadena de bloques de Bitcoin a una transacción fuera de cadena en la Red Lightning.

Con el canal de pago abierto, Mirna puede hacer compras en McDonald's sin tener que abrir un nuevo canal o pagar tarifas altas cada vez. El canal permanece abierto siempre que tanto Mirna como McDonald's quieran usarlo. Por ejemplo, si Mirna compra una hamburguesa por 0.0005 bitcoin, el canal registra que Mirna ahora tiene 0.9995 bitcoin. Y si compra un batido por 0.0003 bitcoin al día siguiente, el canal registra que Mirna ahora tiene 0.9992 bitcoin.

Red Lightning: Utilizando Bitcoin en tu Vida Diaria

Cuando Mirna decide que quiere usar su saldo de bitcoin para otra cosa, cierra el canal transmitiendo una transacción de cierre a la cadena de bloques de Bitcoin. Esto se hace iniciando una transacción de cierre en su Billetera Lightning, y la transacción contiene el saldo final del canal acordado por ambas partes. La transmisión de la transacción a la cadena de bloques de Bitcoin y su confirmación por un minero. Una vez que la transacción se confirma, el canal se cierra y el bitcoin restante en el canal se devuelve tanto a Mirna como a McDonald's.

Es importante tener en cuenta que cerrar un canal puede llevar algún tiempo para confirmarse en la cadena de bloques. Durante este período de espera, los fondos todavía están bloqueados en el canal y no se pueden usar para transacciones en cadena. Mirna recibirá una notificación una vez que se confirme la transacción de cierre. Ahora que hemos configurado nuestra billetera Lightning y hemos leído sobre cómo usar la red Lightning para enviar transacciones, vamos a jugar un juego donde enviamos satoshis (la unidad más pequeña de bitcoin) a otros estudiantes en la clase a través de la red Lightning.

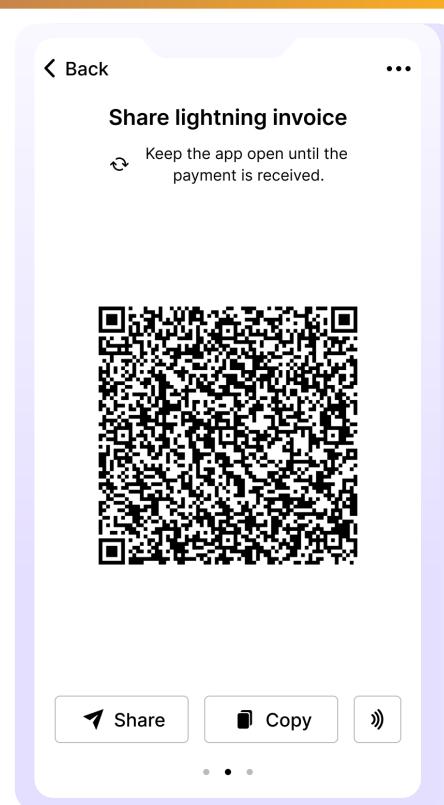


Este es un mapa del mundo entero. Con la Red Lightning, puedes enviar satoshis a cualquier usuario en la red con una Billetera Lightning de Bitcoin. El pago llegará en unos segundos y solo costará unos pocos centavos



Actividad: Ejercicio de Clase: Carrera de relevos con Billeteras Lightning

- 1** Primero, necesitarás descargar una billetera Lightning en tu teléfono o computadora.
- 2** Sigue las instrucciones para instalar la billetera en tu dispositivo en la sección 8.3 de este capítulo.
- 3** Una vez que la billetera esté instalada, ábrela y sigue las indicaciones para configurarla. Esto puede implicar crear una nueva billetera o restaurar una existente, y asegurarla con una contraseña u otra forma de autenticación.
- 4** Genera una factura Lightning, una dirección o un código QR para recibir bitcoin.
- 5** Cuando tu billetera esté configurada y estés listo para recibir satoshis, tu profesor te dará a ti y a tu grupo una cantidad inicial de satoshis enviándolos directamente a tu billetera.

**A**

El objetivo de tu grupo es pasar los satoshis de la billetera de una persona a otra, utilizando la Red Lightning, hasta que lleguen a la última persona del grupo.

B

Para enviar satoshis a otra persona, abre tu billetera y sigue las instrucciones para realizar un pago. Deberás proporcionar la factura Lightning del destinatario o escanear un código QR, e ingresar la cantidad de satoshis que deseas enviar.

C

Si tu grupo es el primero en enviar con éxito los satoshis al último miembro, ¡ganarán! (Y se quedarán con los sats).

Discute las dificultades que tuvo tu grupo con la actividad. ¿Fue fácil, rápido y económico enviar una transacción? ¿Crees que la red Lightning es fácil de usar y entender?

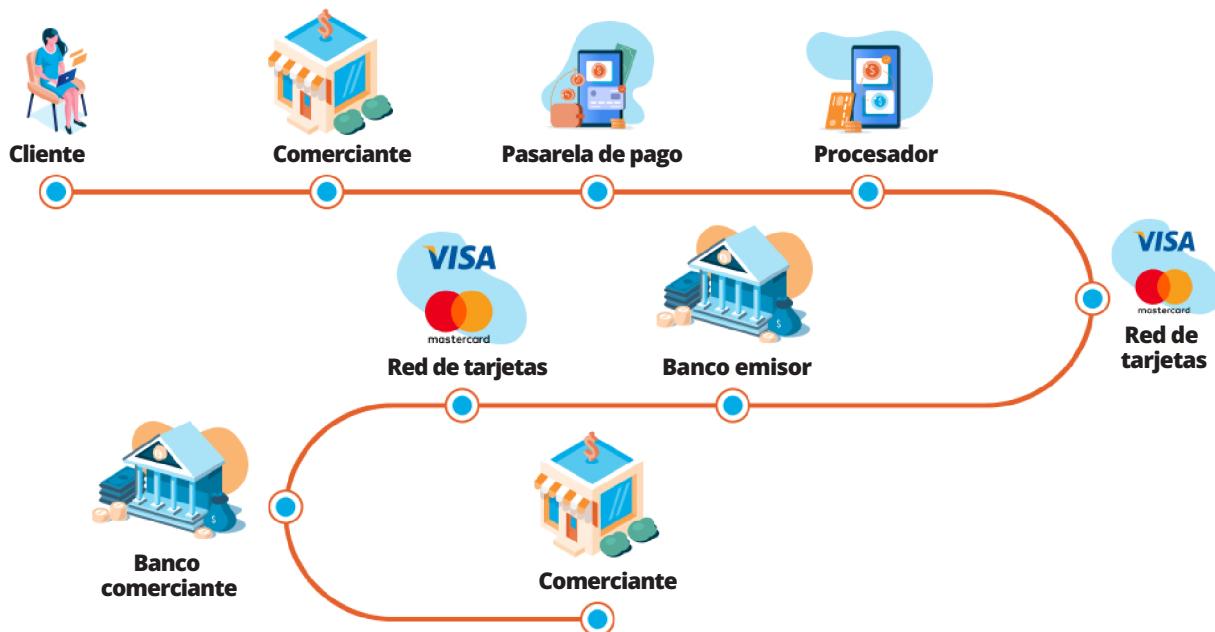
Red Lightning: Utilizando Bitcoin en tu Vida Diaria

8.5 Comprar café y comestibles con bitcoin

¿Alguna vez te has preguntado si podrías usar bitcoin para comprar tu taza diaria de café o abastecerte de comestibles? Resulta que sí se puede. Hay muchas opciones tanto en línea como en persona que te permiten pagar con bitcoin. Exploraremos algunas de esas opciones y herramientas que te ayudarán a encontrar tiendas locales para que puedas gastar bitcoin.

Aunque pagar con una tarjeta de crédito/débito o una aplicación puede parecer fácil de entender para la persona que paga, el procesamiento del pago es mucho más complicado detrás de escena. Hay muchas partes involucradas: el comerciante, su banco, el banco del cliente, la red de tarjetas de crédito y, por supuesto, las tarifas asociadas con cada paso.

Cómo funciona el procesamiento de pagos



Cuando compras cosas, hay muchas partes involucradas y cada parte cobra una tarifa. Para los propietarios de tiendas, estas tarifas pueden ser altas, más del 3% del precio, lo cual es una cantidad grande para ellos.

¡Y eso sin mencionar las tarifas de cambio de moneda!

Tarifas de procesamiento de tarjetas de crédito



Con Bitcoin y la red Lightning, los negocios pueden recibir pagos instantáneos de todo el mundo a través de un sistema monetario abierto, seguro, nativo de Internet, sin fronteras y resistente a la censura.

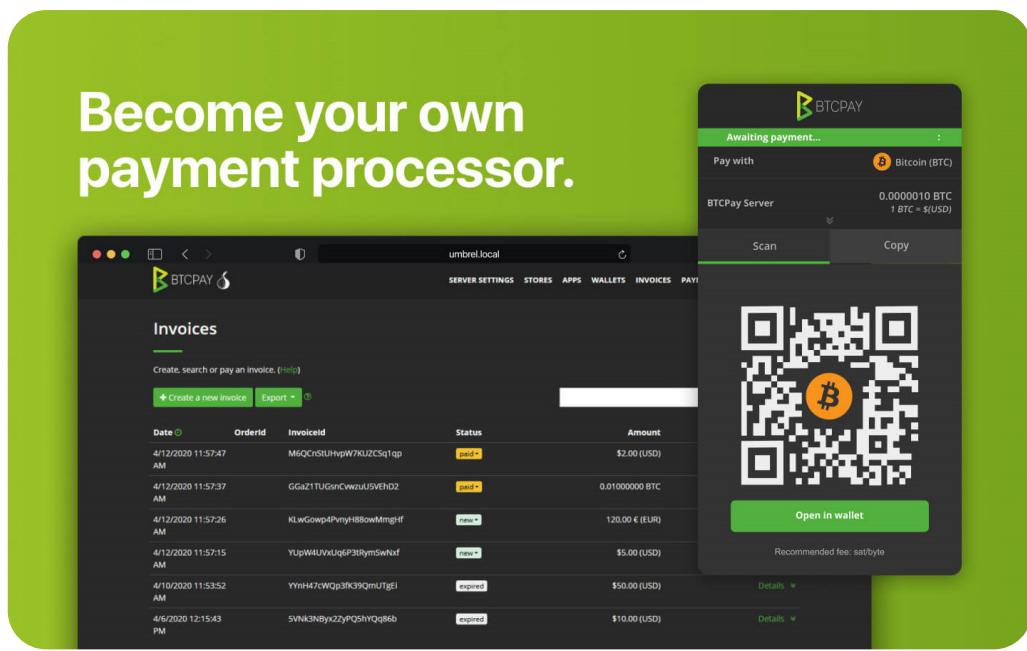
A continuación, veremos algunas formas en que los comerciantes pueden aceptar pagos en bitcoins fácilmente.

8.5.1 En línea: Complementos de pago — Comercio electrónico

BTCPay Server es un procesador de pagos de código abierto que permite a los comerciantes aceptar pagos en bitcoin con poco conocimiento técnico. Es completamente gratuito y no cobra ninguna comisión.

Las empresas en línea pueden integrar BTCPayServer de manera sencilla agregando el complemento BTCPay a su sitio web.

Become your own payment processor.



Red Lightning: *Utilizando Bitcoin en tu Vida Diaria*

Dado que BTCPay Server es un proyecto de código abierto, no una empresa, puedes contribuir al proyecto una vez que aprendas más sobre el proyecto y la programación informática.

Visita BTCPayServer en <https://btcpayserver.org/> para obtener más información sobre cómo utilizar este sistema de pago para tu negocio en persona u en línea.

The infographic is titled "How is it different?" and features the BTCPay Server logo at the top. It is divided into four colored sections: blue, green, yellow, and red. Each section contains an icon and a title, with arrows indicating flow between them.

- Free and open-source**: Shows a hand holding a flower icon. Text: "Made free to free. MIT License. No transaction, subscription or processing costs. Fully open-source. Payments are direct, peer to peer."
- Decentralized**: Shows a network graph icon. Text: "Anyone can deploy a server. Become a self-hosted payment processor and receive payments directly to your wallet. Help your friends or community and process payments for them. An unlimited amount of stores can be attached to a single BTCPay Server."
- Private, No middleman**: Shows two people with a crossed-out arrow icon. Text: "Trusted third parties are security holes. BTCPay eliminates them. Payments are P2P, direct. Data is not shared. There is no KYC / AML"
- Secure**: Shows a padlock with a Bitcoin icon. Text: "Your private key is never required. Non-custodial. BTCPay only needs xpubkey (public key) to generate invoices. Code is open-source and can be inspected by security auditors and developers."
- Censorship-resistant**: Shows a mouth-sealed emoji icon. Text: "No central point of failure. Nobody is controlling it except for the user running it. You can run it on your own hardware."

Icon credits: No Mediator by Arthur Shiron, decentralized by Silvia Santos from the Noun Project

8.5.2 En persona: Encuentra un comerciante en tu área

Las tiendas físicas también pueden utilizar BTCPayServer para aceptar pagos, o simplemente pueden descargar una billetera de Bitcoin y aceptar pagos de Bitcoin directamente desde su teléfono.



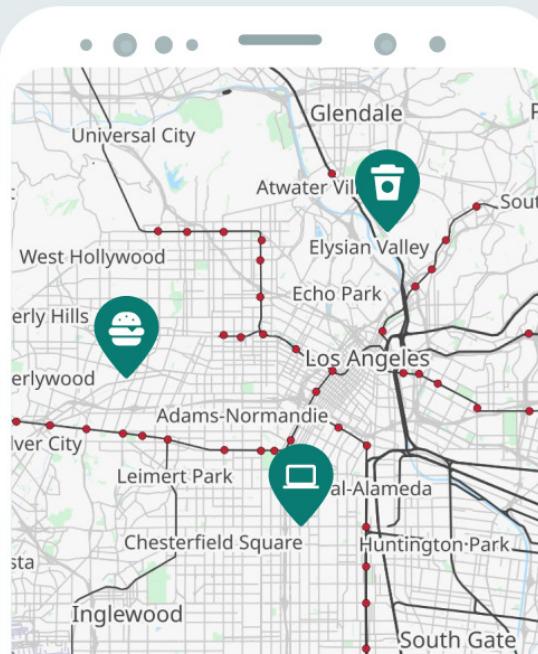


Para encontrar un comerciante que acepte Bitcoin en tu área, visita BTCMap.org y busca tu región.

BTCMap.org es un mapa de código abierto donde los comerciantes que aceptan Bitcoin pueden listar sus negocios. Es una herramienta poderosa para personas que desean gastar sus bitcoins.


BTCMap.org

Easily find places to spend sats anywhere on the planet.



8.5.3 Herramientas de Transición: Vales, Tarjetas de Regalo y Tarjetas de Pago

Para comprar productos o servicios de negocios que aún no aceptan bitcoin, hay una herramienta intermedia que puedes utilizar: las tarjetas de regalo.

Algunos negocios se centran en comprar y vender tarjetas de regalo a cambio de bitcoin. Esto significa que puedes adquirir una tarjeta de regalo para la tienda a la que te gustaría ir a cambio de bitcoin, y luego gastar la tarjeta de regalo directamente en la tienda. ¡Boletos de avión, hoteles, juegos, tarjetas SIM, puedes comprar casi cualquier cosa con bitcoin y tarjetas de regalo!

8.5.4 Economías Circulares y Bitcoin como Medio de Intercambio

El concepto de economía circular proviene de la idea de minimizar el desperdicio en una economía mediante la reutilización y reciclaje de tantos productos y subproductos como sea posible.

Basándose en este concepto, una economía circular de Bitcoin es aquella en la que las transacciones se realizan en bitcoin, y donde el dinero en forma de bitcoin permanece y crece dentro de la economía, beneficiando a sus individuos y empresas.

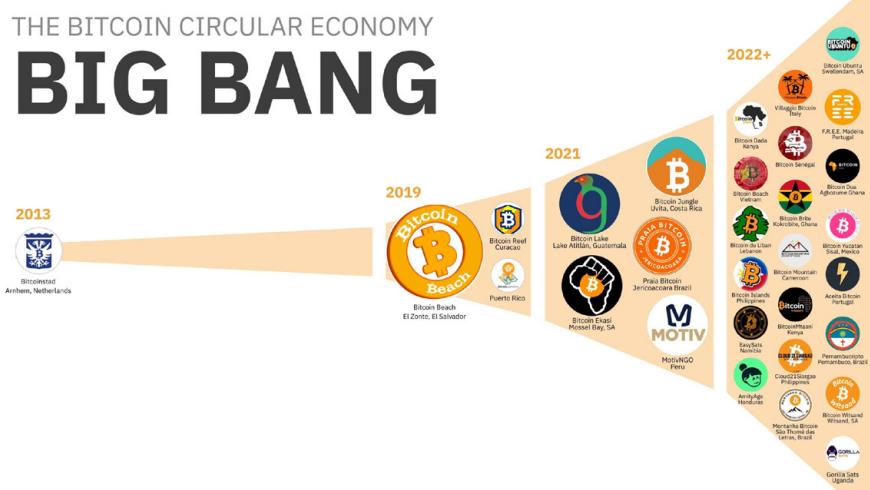


Red Lightning: Utilizando Bitcoin en tu Vida Diaria

La Red Lightning permite que las economías circulares de Bitcoin florezcan en todo el mundo, gracias a transacciones de bitcoin casi instantáneas y con tarifas bajas.



La primera economía circular de Bitcoin creada se encuentra en Arnhem, Países Bajos. Fue creada mucho antes de que existiera la Red Lightning, ¡pero en ese entonces las tarifas en cadena eran realmente bajas!



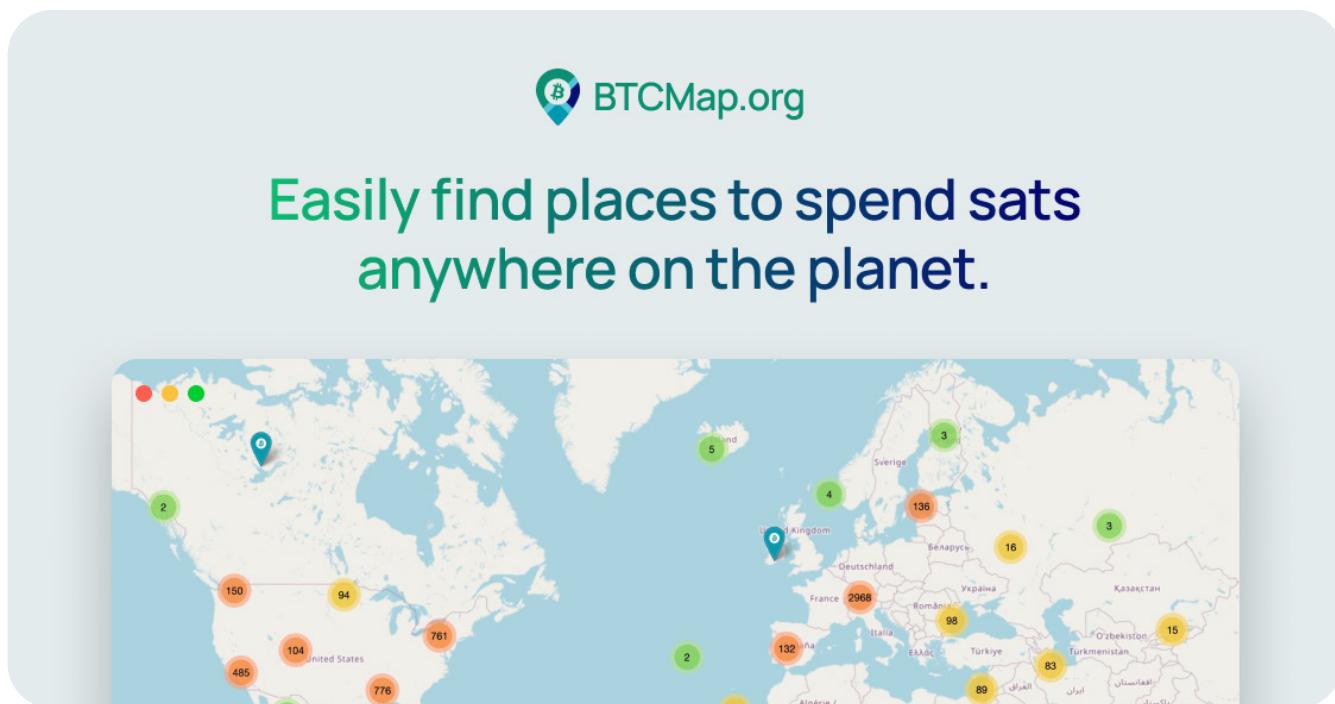
La segunda fue Bitcoin Beach, ubicada en El Zonte, El Salvador. Aprovechó el poder de la Red Lightning para proporcionar a la comunidad, que en su mayoría no tenía acceso a servicios bancarios, pagos digitales instantáneos directamente con sus teléfonos inteligentes.

Hoy en día, cientos de economías circulares están siendo creadas en todo el mundo, impulsadas por Bitcoin, la Red Lightning y recursos educativos.



Capítulo #8

En <https://btcmap.org/> también puedes buscar comunidades de Bitcoin donde conocerás a otros usuarios de Bitcoin y encontrarás negocios que aceptan bitcoin. Algunos de nuestros profesores y estudiantes realmente han agregado negocios y economías circulares a BTCmap.org ¡y una vez que estés listo, tú también puedes hacerlo!



RECURSO: btcmap.org/communities

Al concluir el Capítulo 8, has obtenido información sobre cómo utilizar Bitcoin en tu vida diaria a través de la Red Lightning. La Red Lightning hace que las transacciones sean más rápidas y accesibles, ofreciendo una visión de cómo Bitcoin continuará cambiando y evolucionando en capas.

En el Capítulo 9, investigaremos el lado técnico de Bitcoin. Desde la criptografía hasta los nodos, mineros y más, prepárate para echar un vistazo más de cerca a cómo funciona realmente Bitcoin.

Capítulo #9

Una Introducción al Aspecto Técnico de Bitcoin

9.0 Introducción

Actividad - Ver "Cómo funciona Bitcoin bajo el capó"

9.1 Claves públicas y privadas: Seguridad a través de la criptografía

9.1.1 Criptografía Claves Públicas/Privadas

9.1.2 Explicación del Hashing

Actividad: Generar Hash SHA256

9.2 El modelo UTXO

9.3 Nodos y mineros de Bitcoin

9.3.1 ¿Qué es un nodo de Bitcoin y cómo configuro uno?

Actividad - Ver video sobre nodos de Bitcoin

9.3.2 ¿Qué es un minero de Bitcoin y cómo funciona la minería?

9.4 ¿Qué es el Mempool?

Actividad - Mempool

9.5 Cómo funcionan las transacciones de bitcoin de principio a fin

Actividad - Transacciones de Bitcoin en acción

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

Una Introducción al Aspecto Técnico de Bitcoin

9.0 Introducción



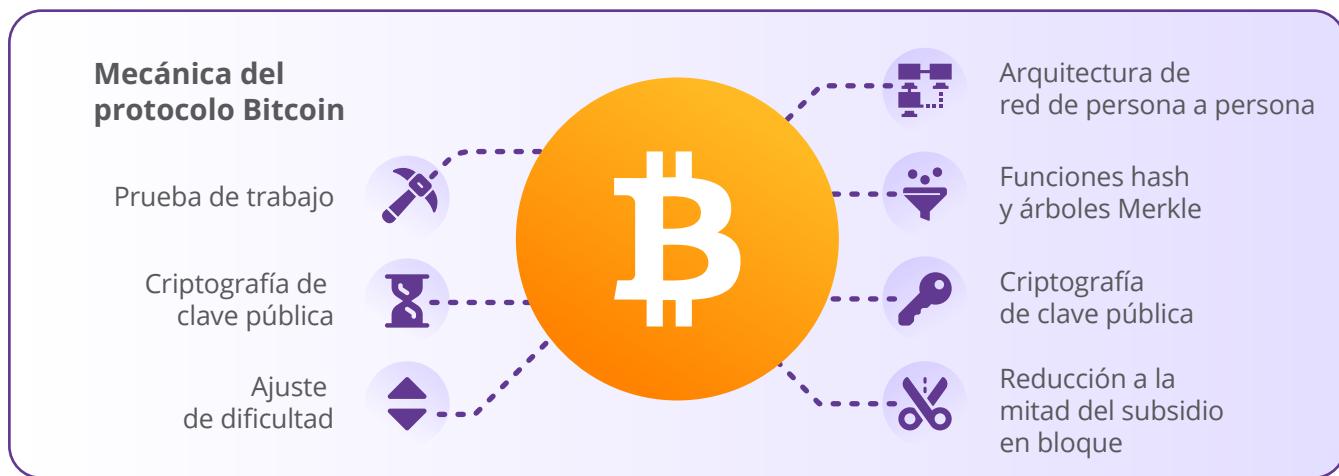
Bitcoin no está "sin regulación", está regulado por su algoritmo en lugar de estar regulado por las burocracias gubernamentales, sin corrupción.

Andreas M. Antonopoulos



En este capítulo, examinaremos más de cerca la tecnología que permite que la Red Bitcoin funcione de manera totalmente descentralizada. Explicaremos de manera sencilla qué sucede cuando envías una transacción de bitcoin, cómo se procesan esas transacciones y qué hacen los mineros y los nodos en la Red Bitcoin.

Vamos a cubrir algunos conceptos desafiantes y técnicos en este capítulo. Algo importante a recordar es que muchas personas no entienden cómo funciona Internet, sin embargo, pueden usarlo todos los días para enviar correos electrónicos, ponerse en contacto con amigos en redes sociales e incluso pagar sus facturas. Aprender el aspecto técnico de cómo funciona Bitcoin es un viaje largo que no todos pueden querer emprender, incluso si deciden usarlo como dinero. Aunque te animamos a seguir aprendiendo sobre los aspectos técnicos de Bitcoin, mantendremos este capítulo centrado en conceptos clave básicos.



Si deseas una comprensión técnica más profunda de cómo funciona Bitcoin, hemos incluido recursos al final de este libro de trabajo. También puedes registrarte en nuestro sitio web para el Bitcoin Diploma - Edición Técnica y recibir notificaciones cuando ese curso más técnico esté listo.

Vamos a empezar viendo un video que muestra cómo funciona la Red Bitcoin.

**Actividad - Ver
"¿Qué es Bitcoin y como funciona?"**



Como viste en el video, la Red Bitcoin es simplemente un libro mayor o registro de transacciones que se almacena en múltiples computadoras llamadas nodos. El libro mayor de Bitcoin es seudónimo, lo que significa que no tiene detalles personales, solo información de transacciones y direcciones. El libro mayor muestra cada bitcoin y sus movimientos desde que la red comenzó el 3 de enero de 2009.

A continuación, examinaremos más de cerca la tecnología que hace posible este sistema..

9.1 Claves públicas y privadas: Seguridad a través de la criptografía

“Lo que Bitcoin nos da es una promesa sólida: el programa se ejecutará exactamente según lo especificado.”

Andreas M. Antonopoulos

9.1.1 Criptografía Claves Públicas/Privadas

La criptografía es una forma de mantener la información en secreto al disfrazarla en código.



El cifrado es el proceso de tomar información y transformarla en un código especial, haciéndola ilegible para cualquiera que no tenga el método correcto de descifrado. Esto es similar a cerrar una caja fuerte, donde solo la persona con la llave o combinación correcta puede abrirla.

La descodificación, por otro lado, es el proceso de tomar la información cifrada y hacerla legible nuevamente, como desbloquear la caja fuerte y poder leer la información dentro.

Por ejemplo, supongamos que Juan quiere enviarle a Arel un mensaje secreto que no está destinado a que nadie más lo lea. Acuerdan usar el método de cifrado de Pigpen para disfrazar el mensaje antes de enviarlo. Solo aquellos con el cifrado pueden descifrar el mensaje, haciéndolo ilegible para cualquier otra persona. Aunque este método no se considera seguro hoy en día, ilustra el principio de la criptografía de clave privada para enviar mensajes.

Cómo resolver

Cifrado de Pigpen

Al resolver el Cifrado de Pigpen, el jugador recibe un mensaje encriptado y un cifrado. Para descifrar el mensaje, el jugador encontrará el símbolo del mensaje encriptado en el cifrado para encontrar la letra descifrada.

“Ejemplo de mensaje cifrado:



A	B	C	J.	K	L	S	W
D	E	F	M.	N	F	T	U
G	H	I	P.	Q	R	V	X

Entonces, ¿cómo funciona la criptografía en las transacciones de bitcoin?

En la criptografía tradicional de clave privada, Juan y Arel tendrían que compartir primero una clave secreta, como una contraseña o el cifrado Pigpen. Luego, Juan usaría esta clave para cifrar su mensaje antes de enviarlo a Arel. Arel, que también conoce la clave secreta, luego usaría la misma clave para descifrar el mensaje y leerlo.

Sin embargo, si alguien más posee la clave e intercepta el mensaje, podría cifrarlo y leerlo.

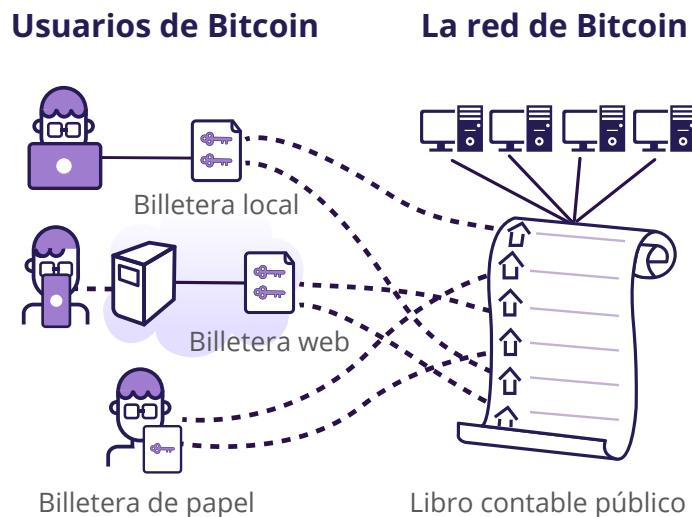
Una Introducción al Aspecto Técnico de Bitcoin

La criptografía de clave pública, el tipo que se utiliza en las transacciones de bitcoin, ha resuelto este problema. Con la criptografía de clave pública, Juan y Arel no necesitan compartir la contraseña o el método de cifrado entre ellos. En cambio, cada uno tiene dos claves diferentes: una clave pública (que es segura para compartir con cualquiera) y una clave privada (que debe mantenerse privada).

En este caso, cuando Juan quiere enviar un mensaje a Arel, puede usar la clave pública de Arel para cifrar su propio mensaje antes de enviarlo a Arel. Cuando Arel recibe el mensaje, solo él puede descifrarlo con su clave privada. Cualquier otra persona, incluso si interceptan el mensaje, no podrá leerlo. Las posibilidades de robar la clave también son mucho menores, porque ni siquiera Juan y Arel necesitan compartir la clave entre ellos.

Entonces, la principal ventaja de la criptografía de clave pública sobre la criptografía de clave privada es que permite una comunicación segura sin la necesidad de que el remitente y el destinatario comparten primero una clave secreta (o otro método de cifrado como Pigpen Cipher), que podría ser interceptada por un tercero.

En Bitcoin, la criptografía de clave pública no se utiliza para enviar mensajes cifrados. En cambio, se utiliza para crear firmas digitales únicas que hacen que las transacciones de bitcoins sean seguras e inmutables. Una firma digital es una forma de demostrar la autenticidad de una transacción de bitcoin, de alguna manera similar a cuando escribes tu firma en un documento físico.



Criptografía de clave pública (Para transacciones entre dos usuarios):

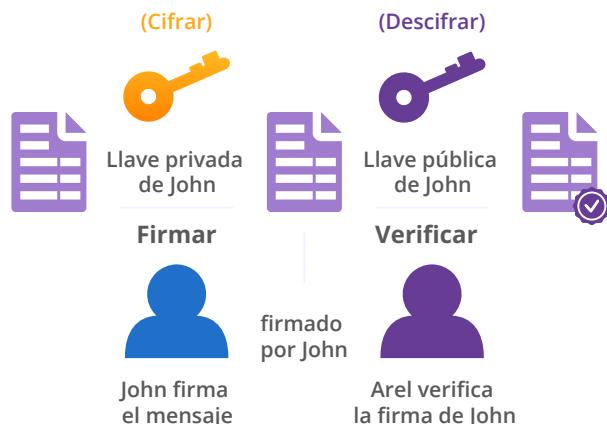
Cada usuario tiene dos claves, una clave privada, que se mantiene en secreto, y una clave pública que puede compartirse con otros.

La clave privada sirve como forma de identificación y prueba de propiedad, confirmando que "esta dirección me pertenece y tengo control sobre ella".

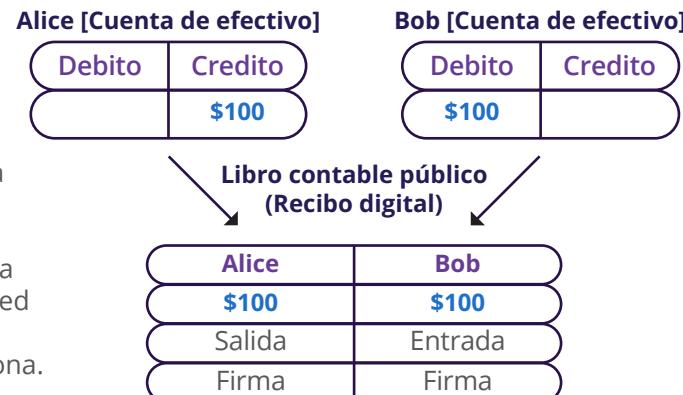
Las firmas digitales se crean para identificar transacciones únicas.



Firma Digital



-  Las transacciones de Bitcoin implican transferir una cierta cantidad de bitcoin directamente a la cuenta de otra persona.
-  Se utiliza cifrado para asegurarse de que solo el verdadero poseedor del bitcoin tenga el control para enviar su dinero a otra persona. Garantiza que la propiedad esté protegida contra actores maliciosos.
-  Como medida adicional de protección, cada transacción que envías en bitcoin recibe automáticamente una FIRMA ÚNICA. Esta firma única está potenciada por tecnología a prueba de manipulaciones que ayuda a la red a verificar que el verdadero propietario del bitcoin ha enviado el bitcoin y no otra persona.



En términos simples, así es como funciona una transacción real de bitcoin:

- 1 Creación de la transacción:**
Un usuario inicia una transacción de bitcoin especificando detalles como la dirección del destinatario y la cantidad de bitcoin a enviar.
- 2 Generación de la firma digital:**
El remitente genera una firma digital única utilizando su clave privada. Esta firma es un código criptográfico único que verifica la autenticidad de la transacción.
- 3 Transmisión de la transacción:**
La transacción firmada se transmite a la red de Bitcoin, indicando la intención de transferir la propiedad del bitcoin del remitente al destinatario.
- 4 Verificación en la red:**
Los nodos en la red de Bitcoin reciben la transacción y utilizan la clave pública del destinatario para desencriptar y verificar la integridad de la transacción. Simultáneamente, utilizan la clave pública del remitente para verificar la firma digital.
- 5 Confirmación en la red de Bitcoin:**
Si la verificación es exitosa, la transacción se añadirá al libro de contabilidad, que sirve como un registro seguro y transparente de todas las transacciones. Una vez confirmada, la propiedad del bitcoin se transfiere oficialmente del remitente al destinatario.



En resumen, la firma digital, creada con la clave privada del remitente, sirve como prueba criptográfica de autenticidad y propiedad, permitiendo que la red descentralizada de Bitcoin valide y registre la transacción en el libro de contabilidad.

Una Introducción al Aspecto Técnico de Bitcoin

9.1.2 Explicación del Hashing

Por favor, no te intimides por los términos técnicos y conceptos matemáticos que vienen a continuación. Entendemos que no a todos les encantan las matemáticas, pero podrías sorprenderte al ver que incluso las ideas más complejas se pueden entender con un poco de esfuerzo.

¿Qué es una función?

Una función es como una máquina que toma cierta información y la convierte en algo nuevo. La información que le das a la función se llama entrada. La nueva información que crea la función se llama salida. Las funciones ayudan a las computadoras a realizar tareas y resolver problemas.



Piénsalo como una receta para hacer una ensalada. La receta (o función) te dice qué ingredientes usar y cómo mezclarlos para hacer la ensalada. Puedes poner ingredientes diferentes, pero la receta siempre te dará la ensalada como resultado. Las funciones se pueden utilizar para hacer las cosas más fáciles y eficientes.

Esta receta, por lo tanto, es una función que toma los ingredientes como entrada y genera la ensalada mezclada como salida.

En Bitcoin, se utilizan funciones para ejecutar transacciones. Ya sabemos que las transacciones en bitcoin son esencialmente transferencias de valor (dinero) de una dirección a otra. Para realizar una transacción, se utilizan varias funciones criptográficas para validar la transacción y actualizar el estado del libro de contabilidad de Bitcoin.

Las funciones utilizadas en una transacción de Bitcoin incluyen verificar la autenticidad de las entradas de la transacción, verificar que el remitente tenga fondos suficientes y actualizar los saldos de las direcciones relevantes. Una vez que una transacción se verifica y se añade a un bloque en el libro de contabilidad, se convierte en parte del registro permanente de todas las transacciones en la red.



¿Qué es una función unidireccional?

Una función unidireccional utiliza un conjunto de instrucciones para procesar la información y convertirla en algo nuevo, como una receta de batido convierte ingredientes en una nueva bebida. Pero, al igual que no puedes deshacer un batido para recuperar los ingredientes originales, no puedes revertir la función unidireccional para obtener la información original de vuelta.



La criptografía de clave pública, de la cual la clave pública es una parte, se basa en el uso de funciones unidireccionales, que dificultan determinar la clave privada a partir de la clave pública. En teoría, no es exactamente "imposible" encontrar la clave privada a partir de la clave pública, pero es extremadamente difícil hacerlo, y llevaría una cantidad desmesurada de tiempo y potencia computacional.

Encontrar una clave privada a partir de una clave pública en Bitcoin es como tratar de encontrar una aguja en un pajar tan grande como un campo de fútbol. La aguja representa la clave privada y el pajar representa todas las posibles claves privadas. De la misma manera, las funciones unidireccionales están diseñadas para ser irreversibles y no se pueden desencriptar.

¿Qué es una función de hash?

Hacer un hash es como tomar una huella digital para datos digitales. Es un proceso de tomar un mensaje digital y convertirlo en un código de longitud fija, que sirve como identificador único.



Al igual que una huella digital puede identificar a una persona, un hash puede identificar un mensaje digital. Los hashes se utilizan en muchas aplicaciones, incluyendo transacciones de bitcoin.

Cómo se utiliza el hash en las transacciones de bitcoin.

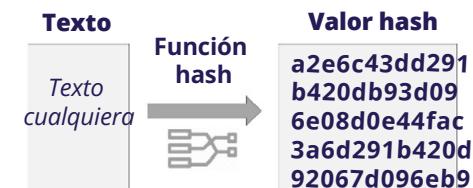
En Bitcoin, cada transacción se hace hash antes de agregarse a un bloque en el libro de contabilidad. El hash actúa como una firma para la transacción, verificando que la transacción es válida y no ha sido manipulada. Si alguien intenta cambiar incluso una sola letra en la transacción, el hash será completamente diferente, alertando a otros sobre el cambio.

El papel del hash en proporcionar seguridad

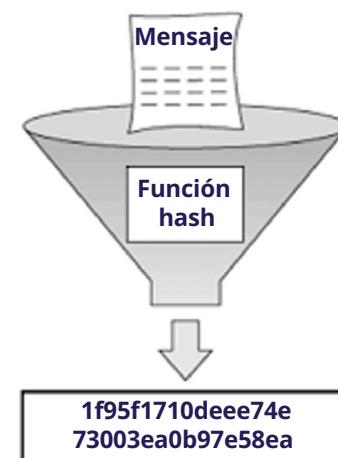
El hashing es esencial para la seguridad de la Red Bitcoin. Al utilizar hashes para identificar transacciones, la red puede detectar cualquier intento de cambiar o manipular una transacción. Esto ayuda a prevenir el fraude y asegura que todas las transacciones se registren con precisión en el libro de contabilidad.

Una función de hash es un tipo de función unidireccional que toma una entrada (llamada "mensaje" o "datos") y la convierte en una representación numérica llamada "hash". El hash de salida es único para los datos de entrada, por lo que incluso un pequeño cambio en los datos de entrada resulta en un hash completamente diferente.

Una función de hash es como una máquina de códigos secreta. Toma un mensaje y lo convierte en un código.

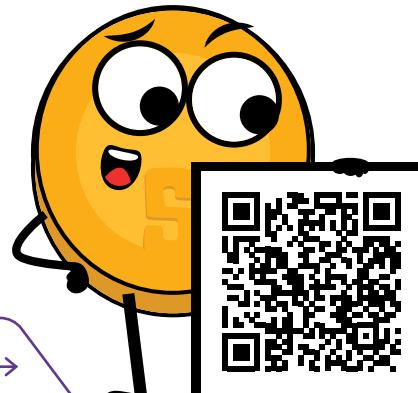


Datos de longitud arbitraria



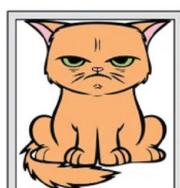
Una Introducción al Aspecto Técnico de Bitcoin

El código siempre se ve igual para el mismo mensaje. Si cambias el mensaje aunque sea un poco, el código será completamente diferente. Esto ayuda a las computadoras a recordar cosas y verificar si algo ha cambiado.



Genera instantáneamente un hash SHA256 de cualquier cadena o valor de entrada. Las funciones hash se utilizan como métodos unidireccionales.

Actividad - Generar Hash SHA-256



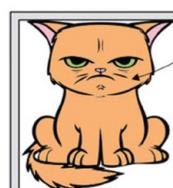
Entrada
cat.jpg 1.21MB



A 32-byte hash

e40326f7aa7305
500fea0a9a2b43
9ebea93827ba21
039404439fe33e

¡Le falta un bigote!
Ahora tiene una razón para estar gruñona



Entrada
cat.jpg 1.21MB



A 32-byte hash

664eaa3b78f7aa
7305890e3aab53
22a0a9a2048bef
4f8342048b90e3

Completamente diferente al hash anterior

La salida, o hash, siempre tiene la misma longitud, no importa cuánto tiempo fuera la información original. Bitcoin utiliza algunos tipos específicos de funciones de hash llamadas SHA-256 y RIPEMD160. Algunos ejemplos a continuación:

💡 Observa que un pequeño cambio en la segunda entrada cambia completamente la salida en comparación con la primera.

💡 La tercera entrada es un archivo enorme pero la salida sigue siendo la misma longitud fija que las otras dos.

El hashing también se puede pensar como una partitura musical que captura la esencia de una pieza musical. Al igual que una partitura musical es una representación única de una melodía, un valor hash es una representación única de un conjunto de datos. Al comparar la partitura de una pieza musical con la interpretación real, un músico puede determinar si la interpretación es precisa. De manera similar, al comparar el valor hash de los datos recibidos con el valor hash original, se puede determinar si los datos han sido alterados durante la transmisión.

El valor SHA256 de hello world
B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcded

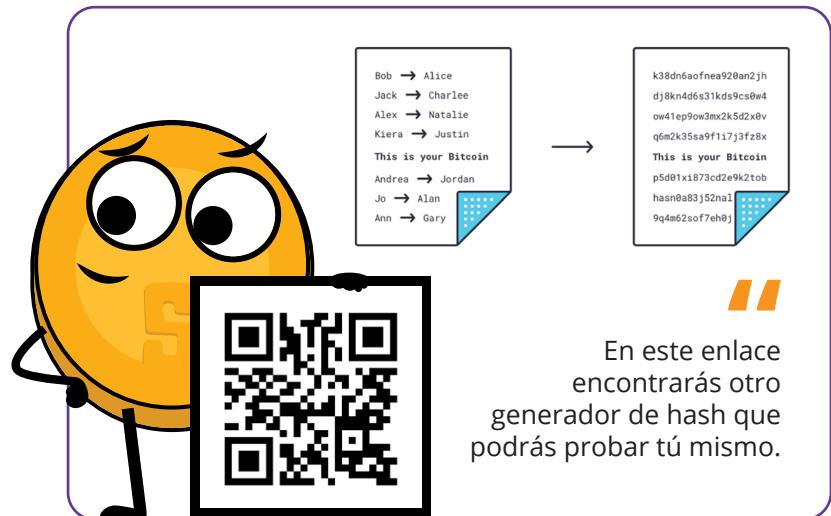
The SHA256 value of "hello world."
7ddb22731 5f423250fc67f3be69c544628dff41752af91 c50aeQa9c49faeb87

El valor SHA256 de un archivo .ISO grande "Ubuntu 24.04"
7b9f670c749f797a0f7481d61 9ce8807edac052c97e1 a0df3b130c95efae4765



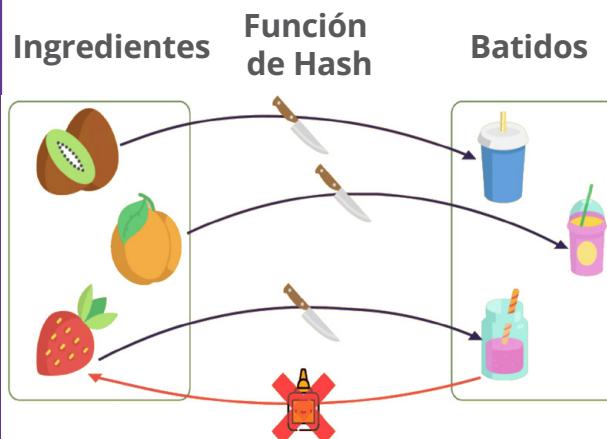
Del mismo modo que una ligera desviación en una actuación musical puede hacer que suene diferente, incluso el cambio más mínimo en los datos originales resultará en un valor hash diferente. Esto hace que la función de hash sea una herramienta poderosa para garantizar la integridad y autenticidad de una transacción de bitcoin.

El proceso de codificación de la clave pública mediante la función de hash se utiliza para mejorar la seguridad de la información al convertirla en un formato de longitud fija e ilegible. Bitcoin utiliza los algoritmos SHA-256 y Ripemd-160 para producir direcciones públicas. La salida resultante sirve como un identificador único para la clave pública y contribuye a garantizar la integridad y seguridad de las transacciones almacenadas en el libro contable. Al cifrar la información de esta manera, se dificulta que personas no autorizadas accedan y manipulen los datos.



Hashing

Una función hash toma cualquier entrada y produce una salida de longitud fija (hash).



Determinista.

Con los mismos ingredientes siempre se obtiene el mismo batido.

Resistencia previa a la imagen.

No puedes pegar una fresa cuando te dan un batido.

Resistencia a la correlación.

Cambiando un poco los ingredientes se obtiene un batido completamente diferente.

Resistencia a la colisión.

Es difícil encontrar ingredientes diferentes para un batido que resulten exactamente en el mismo

Velocidad y verificabilidad.

Arroja frutas en la licuadora. Es rápido y lo que sale seguro es un batido.

9.2 El Modelo UTXO

UTXO significa Salida de Transacción No Gastada

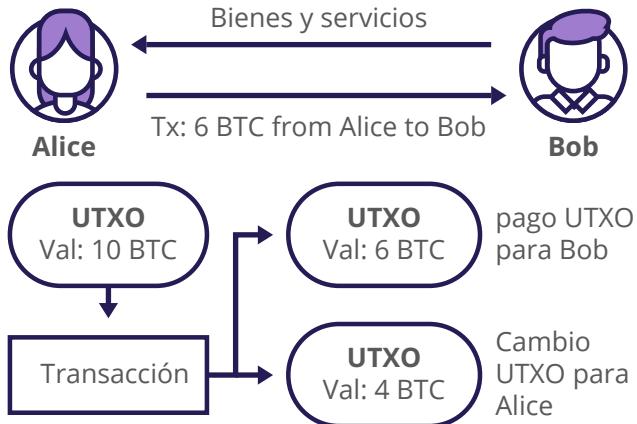


Una Introducción al Aspecto Técnico de Bitcoin

¿Qué son UTXOs?

En Bitcoin, las transacciones funcionan como dividir una pieza más grande de oro en piezas más pequeñas y enviar estas piezas más pequeñas tanto a otros como a ti mismo.

Puedes pensar en los UTXOs como diferentes tamaños y piezas de bitcoin, o billetes denominados de manera diferente en tu billetera. Cuando gastas un UTXO, se recrea en un nuevo UTXO para el receptor, y lo que queda se te devuelve en un nuevo UTXO diferente conocido como el "cambio UTXO". Esto es similar a usar un billete de \$10 para comprar dos tazas de café por \$6. La cafetería conserva la pieza de \$6 y te devuelve \$4 de cambio.



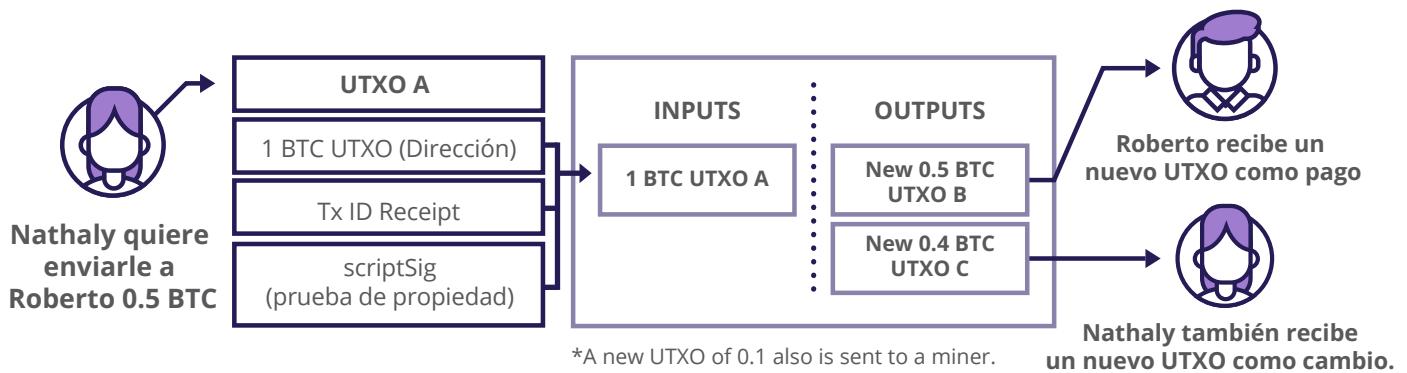
Cuando envías bitcoin, siempre envías la cantidad completa de uno (o más) de tus UTXOs en tu billetera de Bitcoin. ¿Qué sucede? Envías una parte al destinatario, y recibes la cantidad restante de vuelta como cambio a una de tus nuevas direcciones de Bitcoin. El cambio que recibes se llama salida de transacción no gastada, o UTXO, y se puede utilizar como entrada para una nueva transacción futura.

El saldo de tu billetera de Bitcoin es la suma de todos tus UTXOs diferentes. Entonces, la suma de tus UTXOs es la suma de la cantidad de bitcoin que posees.



Es importante tener en cuenta que no debes hacer que otros conozcan tus UTXOs, porque cuando alguien conoce tus UTXOs, puede rastrear tus transacciones de bitcoin en la red y, en última instancia, sabrá cuánto dinero posees

En conclusión, cada vez que realizas una transacción, utilizas uno o más de tus UTXOs existentes para gastar bitcoin, y se crean nuevos UTXOs (tanto para ti como receptor).



Cuando se realiza una transacción, la cantidad de bitcoin que se envía se divide en múltiples salidas, cada una de las cuales está asociada con una nueva dirección de Bitcoin (un nuevo UTXO).



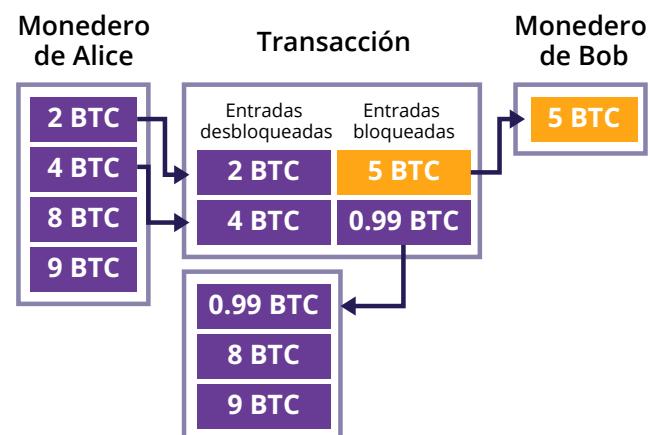
Al enviar bitcoin a alguien, usarás uno o más UTXOs como fuente de los fondos (entrada). Estos UTXOs se combinarán, si es necesario, para crear nuevas salidas que pertenecen tanto al destinatario de la transacción como a ti mismo. Estas nuevas salidas, o UTXOs, luego se convierten en propiedad del destinatario y tuya. Estos UTXOs luego se pueden usar como fuente de fondos en otras transacciones futuras. Esta cadena de UTXOs crea un historial transparente y rastreable de todas las transacciones de bitcoin en el libro contable de Bitcoin, comenzando desde el primer bloque (3 de enero de 2009).

Un ejemplo para ilustrar cómo funciona esto: si quieres enviar 2 bitcoin pero solo tienes un UTXO de 5 bitcoin, la diferencia de 3 bitcoin se te envía de vuelta como "cambio". Este cambio es un nuevo UTXO para ti, y puedes gastar ese nuevo UTXO en una transacción futura.

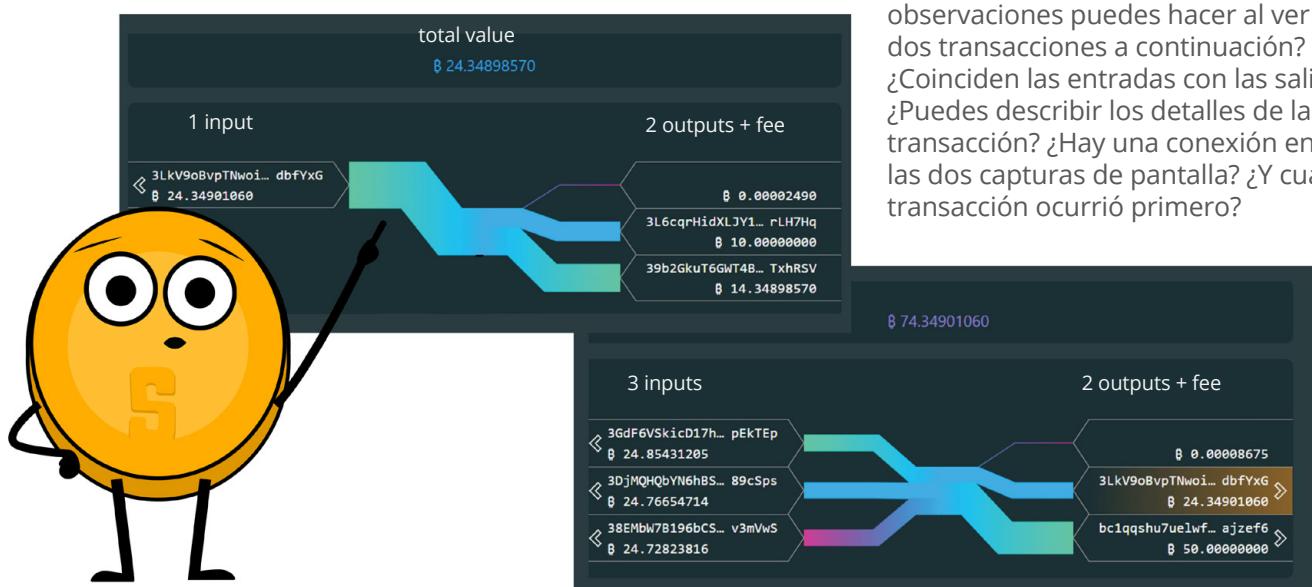
Otro ejemplo:

- 1** Alice quiere enviar a Bob 5 bitcoin.
- 2** Combina 6 bitcoin de dos de sus UTXOs.
- 3** De estos UTXOs, envía 5 bitcoin a Bob, recibe 0.99 bitcoin como cambio de vuelta y necesita pagar una tarifa de transacción de 0.01 bitcoin.
- 4** Después de la confirmación, la transacción se agrega al libro contable de Bitcoin, actualizando todos los nodos que tienen una copia del libro contable.

Si Alice intentara usar una de sus salidas ya gastadas para hacer otra transacción, sería automáticamente rechazada por los nodos. Esto se debe a que los nodos mantienen una copia del libro contable de Bitcoin (y todas sus transacciones), por lo que pueden verificar fácilmente el saldo de los UTXOs de Alice y comprobar que la transacción no es válida.



A continuación, se muestra una captura de pantalla real de una transacción donde solo hay una entrada. Sin embargo, el saldo inicial podría, en otro caso, ser la suma de múltiples UTXOs (múltiples entradas). ¿Qué observaciones puedes hacer al ver las dos transacciones a continuación? ¿Coinciden las entradas con las salidas? ¿Puedes describir los detalles de la transacción? ¿Hay una conexión entre las dos capturas de pantalla? ¿Y cuál transacción ocurrió primero?



Una Introducción al Aspecto Técnico de Bitcoin

9.3 Un vistazo más cercano a los Nodos y Mineros de Bitcoin

En esta sección, vamos a examinar de manera más detallada dos partes (y participantes) muy importantes de la Red de Bitcoin que fueron introducidas por primera vez en el Capítulo 6. Vamos a analizar:

1

Nodos de Bitcoin:

Guardianes de la validación cuyo trabajo principal es mantener una copia del libro contable de Bitcoin, asegurarse de que todas las transacciones sean válidas y de que todos sigan las mismas reglas. Al distribuir esta tarea entre muchas personas en todo el mundo, Bitcoin se mantiene fuerte frente a posibles problemas. Estos Nodos ayudan a mantener el sistema confiable y fiel a su idea descentralizada, donde ninguna persona o grupo tiene demasiado poder.

2

Mineros de Bitcoin:

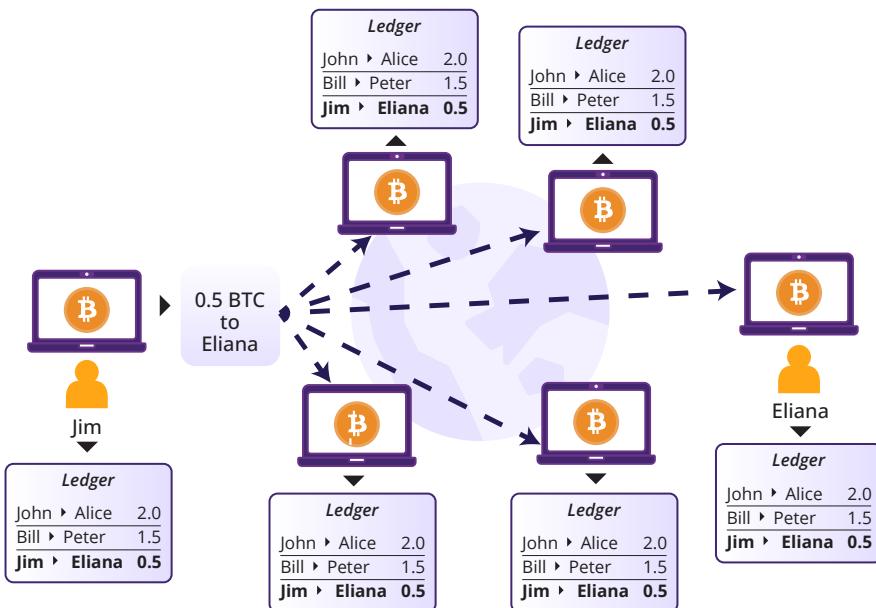
Arquitectos de la Seguridad que utilizan potentes computadoras y electricidad para verificar y confirmar transacciones, asegurándose de que todo sea seguro. Este trabajo ayuda a que el libro contable, o blockchain, sea resistente a cualquier actor malintencionado que intente alterar las cosas.

Juntos, los nodos de Bitcoin y los mineros trabajan como un equipo para mantener un sistema descentralizado, seguro y fuerte: una nueva forma de manejar el dinero en la que personas de todo el mundo pueden confiar. Vamos a explorar estos roles con más detalle para entender cómo contribuyen al innovador sistema de Bitcoin.

9.3.1 ¿Qué es un Nodo de Bitcoin y cómo lo configuro?

Un nodo de Bitcoin puede sonar técnico, pero es simplemente un software que ejecuta una copia del libro contable de Bitcoin. Cuando ejecutas tu propio nodo de Bitcoin, obtienes voz en la formación de las reglas de la red de Bitcoin.

Imagina esto: si un grupo de personas intenta cambiar cómo funciona Bitcoin, por ejemplo, alterando el suministro total de Bitcoin, tienes voz. Puedes optar por no cambiar tu nodo al nuevo sistema, lo que es como votar para hacer cumplir las reglas de la red que respaldas.



Pensemos en un Nodo de Bitcoin como un policía de tráfico digital con algunas tareas esenciales:

Guardianes de la Validación:

1

Un Nodo de Bitcoin mantiene una copia digital del blockchain, que es como un libro mayor compartido de todas las transacciones de bitcoin. Muchos nodos alrededor del mundo tienen este mismo registro.

2

Centro de Comunicación:
Los nodos se conectan entre sí, creando una vasta red de comunicación. Comparten información, especialmente transacciones que esperan ser agregadas al blockchain, almacenadas en una sala de espera digital llamada "mempool."

3

Verificador de Calidad:
Cada adición al blockchain se somete a escrutinio. Los nodos aseguran que las transacciones sean válidas, rechazando aquellas que no cumplen con las reglas de la red de Bitcoin.

4

Informante del Blockchain:
Otro software, como las billeteras, puede solicitar a un nodo información sobre el blockchain, como saldos de bitcoin. Los nodos sirven como centros de información.

5

Bienvenida a nuevos nodos:
Cuando un nuevo nodo quiere unirse, los nodos existentes proporcionan generosamente una copia del blockchain. El nuevo nodo verifica de manera independiente la validez de cada transacción, enfatizando un sistema sin confianza.

Actividad - Ver video sobre nodos de Bitcoin



Una de las opciones para ejecutar tu propio nodo es descargar el software Bitcoin Core y darle tiempo para descargar todo el blockchain. Una vez listo, puedes dejarlo encendido y, aproximadamente cada 10 minutos, llegan nuevos bloques con transacciones. Tu nodo verifica su validez, añadiéndolos a tu copia local del blockchain.

Recurso:
Software
Bitcoin Core



Ejecutar o correr un nodo proporciona soberanía e independencia. No dependes de otros; es tu propio policía de tráfico. A diferencia de tu billetera de Bitcoin, que carece de una copia del blockchain, un nodo garantiza autosuficiencia. En lugar de confiar en otros sobre tus tenencias de bitcoin (y el estado de la red de Bitcoin), tu billetera se comunica con tu nodo personal, haciendo tu experiencia digital más segura y confiable.

9.3.2. ¿Qué es un minero de Bitcoin y cómo funciona la minería?

El propósito de la minería no es la creación de nuevos bitcoin; ese es el sistema de incentivos. La minería es el mecanismo por el que se descentraliza la seguridad de Bitcoin.

Andreas M. Antonopoulos

Una Introducción al Aspecto Técnico de Bitcoin

Los mineros recopilan transacciones no confirmadas, forman un bloque y gastan energía buscando una clave valiosa que agregará y asegurará el lugar del bloque en la blockchain.



Los mineros compiten para agregar el siguiente bloque a la blockchain. El premio buscado es un "hash de bloque válido", astutamente oculto entre miles de millones de otros, y solo una clave específica asignada por la red puede desbloquearlo. Imagina un enorme montón de heno lleno de millones de claves, cada una representando un hash único de bloque. La red ha elegido una clave específica para desbloquear una recompensa valiosa. Los mineros rebuscan en el montón, probando cada clave en la cerradura, pero solo un afortunado minero descubrirá la combinación perfecta. Una vez que un minero encuentra el hash de bloque correcto, lo comparte con la red junto con su bloque recién creado de nuevas transacciones. Otros mineros verifican la solución para asegurarse de que sea la adecuada. Si todo está en orden, el bloque se agrega al blockchain, creando un libro mayor seguro y público.

Los mineros obtienen recompensas por sus esfuerzos de dos maneras:

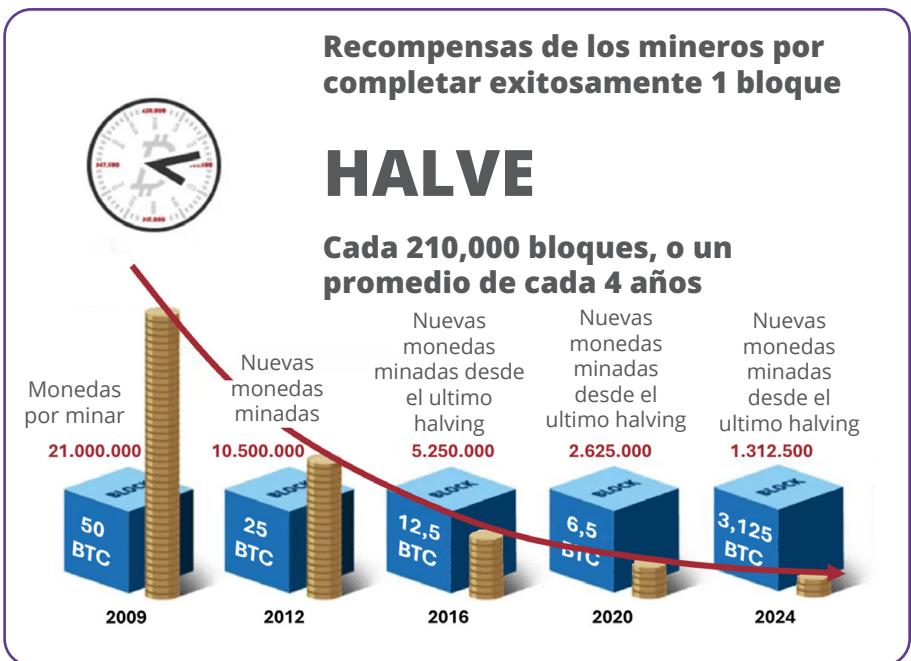
1 Recompensa por Bloque

2 Comisiones por transacción

Las recompensas por bloques son nuevos bitcoins liberados en circulación con cada bloque agregado al blockchain. Las tarifas de transacción son pequeños pagos en bitcoin que los usuarios hacen para que sus transacciones se procesen más rápido y sean priorizadas por el minero. Los mineros pueden elegir qué transacciones incluir en el bloque que minan, dando preferencia generalmente a aquellas con tarifas de transacción más altas.

Halving de Bitcoin

Un halving de Bitcoin es una parte esencial del universo de Bitcoin que ayuda a mantener su escasez y valor con el tiempo. Como sabes, hay un suministro fijo de 21,000,000 bitcoins en total. Este suministro no está disponible por completo desde el día en que Bitcoin se lanzó. En su lugar, este suministro entra al universo de Bitcoin de manera gradual. Satoshi Nakamoto diseñó astutamente un sistema de recompensa por bloque para distribuir nuevos bitcoins sin una autoridad central. En los primeros días de Bitcoin, los mineros obtenían una jugosa recompensa de 50 bitcoins por cada bloque que minaban, motivándolos a invertir en equipos potentes y electricidad para sus operaciones mineras.



Para mantener la estabilidad de la red y gestionar el nuevo suministro de bitcoin, la recompensa por bloque se reduce a la mitad aproximadamente cada 210,000 bloques. Este evento, llamado "el halving", disminuye la cantidad de nuevos bitcoins que entran en circulación y continúa motivando a los mineros a proteger la red y mantener su descentralización. Históricamente, los eventos de halving han llevado a aumentos significativos en el precio del Bitcoin debido a la reducción en la oferta de nuevos bitcoins que ingresan a la circulación.

El suministro en Circulación se refiere a la cantidad total de una moneda. Con bitcoin, el suministro en circulación total es el número de monedas que se han minado y están en circulación en un momento dado, excluyendo las monedas que se han perdido para siempre.

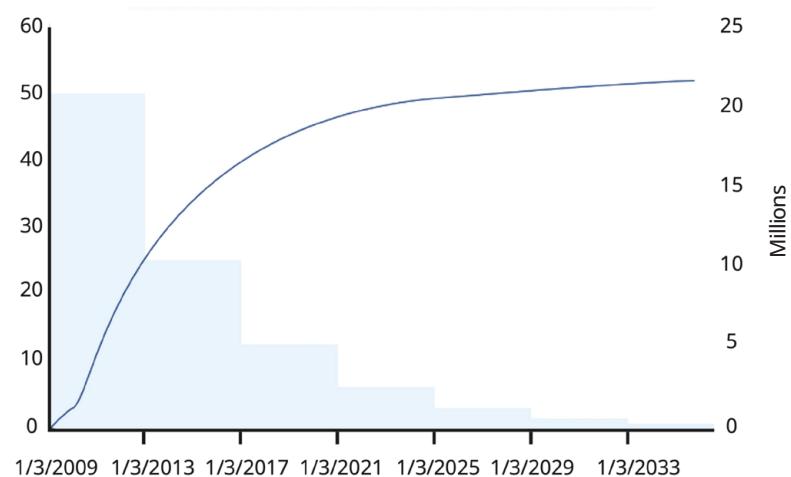
Durante cada evento de halving, los mineros reciben menos recompensas en bitcoins, lo que reduce la tasa de emisión de nuevas monedas. Como resultado, la dificultad de minería de Bitcoin aumenta para mantener un tiempo de bloque de aproximadamente 10 minutos, asegurando que se agreguen nuevos bloques al blockchain a un ritmo constante. La reducción en las recompensas de minería no significa necesariamente que los mineros ganen menos beneficios, ya que también pueden ganar tarifas de transacción por verificar transacciones y agregarlas al blockchain, lo que puede compensar la disminución en las recompensas de minería. Los eventos de halving están programados previamente en el protocolo de Bitcoin, lo que hace que el cronograma de suministro de Bitcoin sea predecible y transparente.



El cronograma de suministro de bitcoin es el plan predeterminado y público para la liberación de nuevos bitcoins en circulación, diseñado para mantener la escasez de bitcoin con el tiempo.

La siguiente tabla describe los detalles de los próximos eventos de halving para Bitcoin, incluida la fecha esperada del próximo evento de halving, el número de bloque en el que ocurrirá el evento de halving, las recompensas por bloque (por bloque minado) durante ese evento de halving y el porcentaje del suministro total que se minará.

Cronograma de suministro de Bitcoin



Evento	Fecha prevista	Bloque	Recompensa por bloque	Porcentaje minado
Cuarto Halving	2024	840,000	3.125	96.875 %
Quinto Halving	2028	1,050,000	1.5625	98.4375 %
Sexto Halving	2032	1,260,000	0.78125	99.21875 %

Una Introducción al Aspecto Técnico de Bitcoin

A medida que se mina más bitcoin, el suministro en circulación y el porcentaje del suministro total que se ha minado seguirán aumentando hasta alcanzar el suministro total de 21,000,000. La reducción en el suministro, combinada con la creciente demanda, puede impulsar el precio del Bitcoin (medido en dólares). Esto beneficia a los primeros adoptantes y también motiva a los mineros a continuar asegurando la red y contribuyendo con su potencia informática y recursos.

Bitcoin: porcentaje de suministro de 21 millones minados

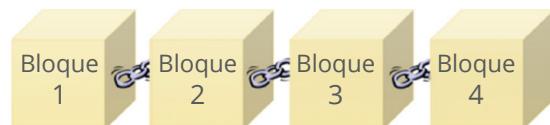


¿Qué es un hash de bloque válido en Bitcoin?

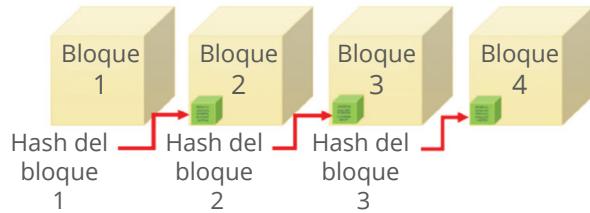
En Bitcoin, un hash de bloque válido es como un código especial que los mineros intentan encontrar. Es un número único que ayuda a realizar un seguimiento de cada bloque en el blockchain, que almacena información sobre transacciones. Los bloques se conectan en una cadena desde el primero (bloque génesis) hasta el más reciente, creando un registro público de todas las transacciones. Este hash de bloque es crucial porque vincula cada bloque al anterior, facilitando que cualquiera verifique el historial de transacciones. Es un poco como una huella dactilar para cada bloque, asegurando que la información sea correcta y segura. El hash de bloque actúa como una forma de confirmar que los datos en el bloque no han sido modificados.



9ebtsznmfs7l4b876c5i 7vo3bbv6kq4gem4ywzpu



Los bloques están "vinculados" entre sí mediante la aplicación de una relación específica entre los bloques. Es decir, un bloque debe contener una "huella digital", que es un valor hash de los datos del bloque anterior. Una función hash puede condensar un mensaje arbitrario (la información del bloque) a un tamaño fijo (por ejemplo, 160 bits) y produce una huella digital del mensaje.



Satoshi Nakamoto, el creador de bitcoin, minó el bloque inicial, que contenía un total de 50 bitcoins.

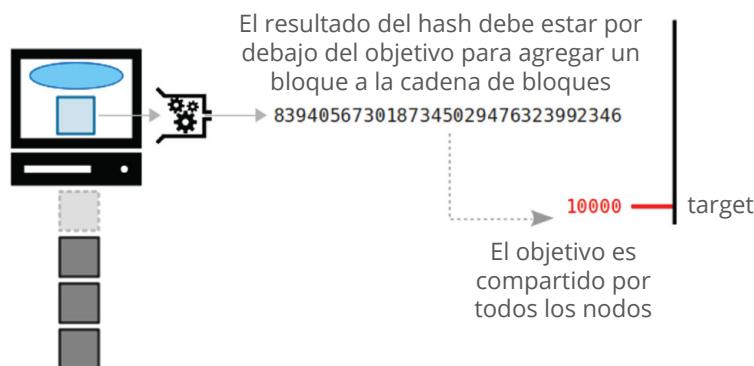


Capítulo #9

La carrera para minar un bloque

Los mineros participan en una competencia para descubrir el hash de bloque que se alinea con el objetivo (un número especial) establecido por la red. El minero que sea el primero en descubrir con éxito el hash de bloque correcto tiene la oportunidad de agregar ese bloque al blockchain y asignarle el ID de hash correspondiente. Esta solución sirve como validación de la autenticidad del bloque.

La minería se puede comparar con una carrera donde el objetivo es llegar a la meta lo más rápido posible. La dificultad para encontrar el hash de bloque se ajusta periódicamente, asegurando que cada bloque siga siendo minado en aproximadamente 10 minutos (a medida que los mineros se unen y se van). Este mecanismo se llama el "ajuste de dificultad".



Supongamos que el número objetivo establecido por la red de Bitcoin es 1000. Los mineros tendrían que utilizar su potencia computacional y energía para buscar un hash de bloque (un número específico) que sea menor que 1000. El primer minero en encontrar un hash de bloque que sea menor que 1000 tiene la oportunidad de agregar el nuevo bloque al blockchain y recibe una recompensa en bitcoin.



El nivel de dificultad en la minería de Bitcoin es una medida de cuán difícil es encontrar un hash de bloque válido que cumpla con el objetivo establecido por la red. Se ajusta cada 2016 bloques, o aproximadamente cada dos semanas, para asegurar que los bloques se agreguen al blockchain a una tasa consistente. El nivel de dificultad se expresa como un número y cuanto más alto sea el nivel de dificultad, más difícil será encontrar un hash de bloque válido.

Por ejemplo, considera dos hashes diferentes:

- ◆ **Hash 1:** 0000A1mNgF0RbL0cK5wltHth3hAy5tAcK
Nivel de dificultad: 1
- ◆ **Hash 2:** 00000000A1mNgF0RbL0cK5wltHth3hAy5tAcK
Nivel de dificultad: 2

En este ejemplo, Hash 2 tiene un nivel de dificultad más alto que Hash 1, porque es un hash más largo con más ceros al principio. Sería más difícil para los mineros encontrar Hash 2 porque sus computadoras necesitarían hacer más trabajo.



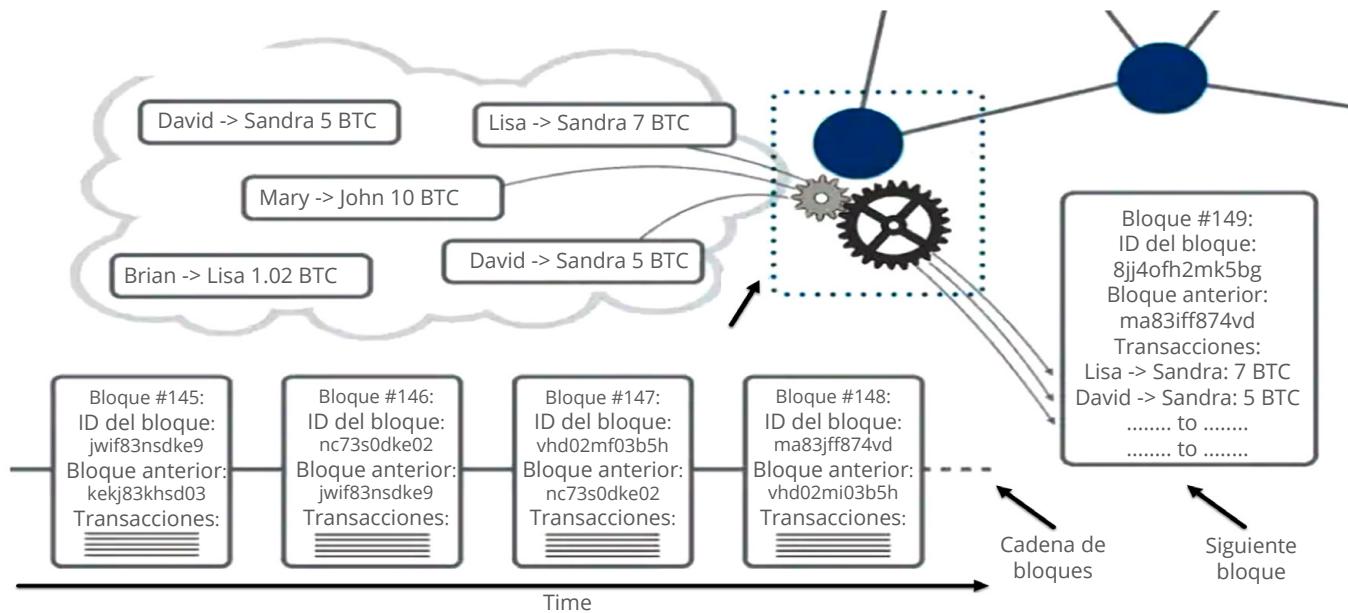
Al encontrar un hash de bloque válido, un minero demuestra que ha realizado el trabajo necesario para agregar el nuevo bloque al blockchain y recibe una recompensa en bitcoin, además de tarifas de transacción por su esfuerzo. La Prueba de Trabajo (PoW) es el método que utiliza la Red de Bitcoin para validar transacciones y agregar nuevos bloques al blockchain.

Una Introducción al Aspecto Técnico de Bitcoin

PoW mantiene segura a Bitcoin al dificultar que cualquiera con intenciones maliciosas tome el control.

En resumen, las tareas de los mineros consisten en:

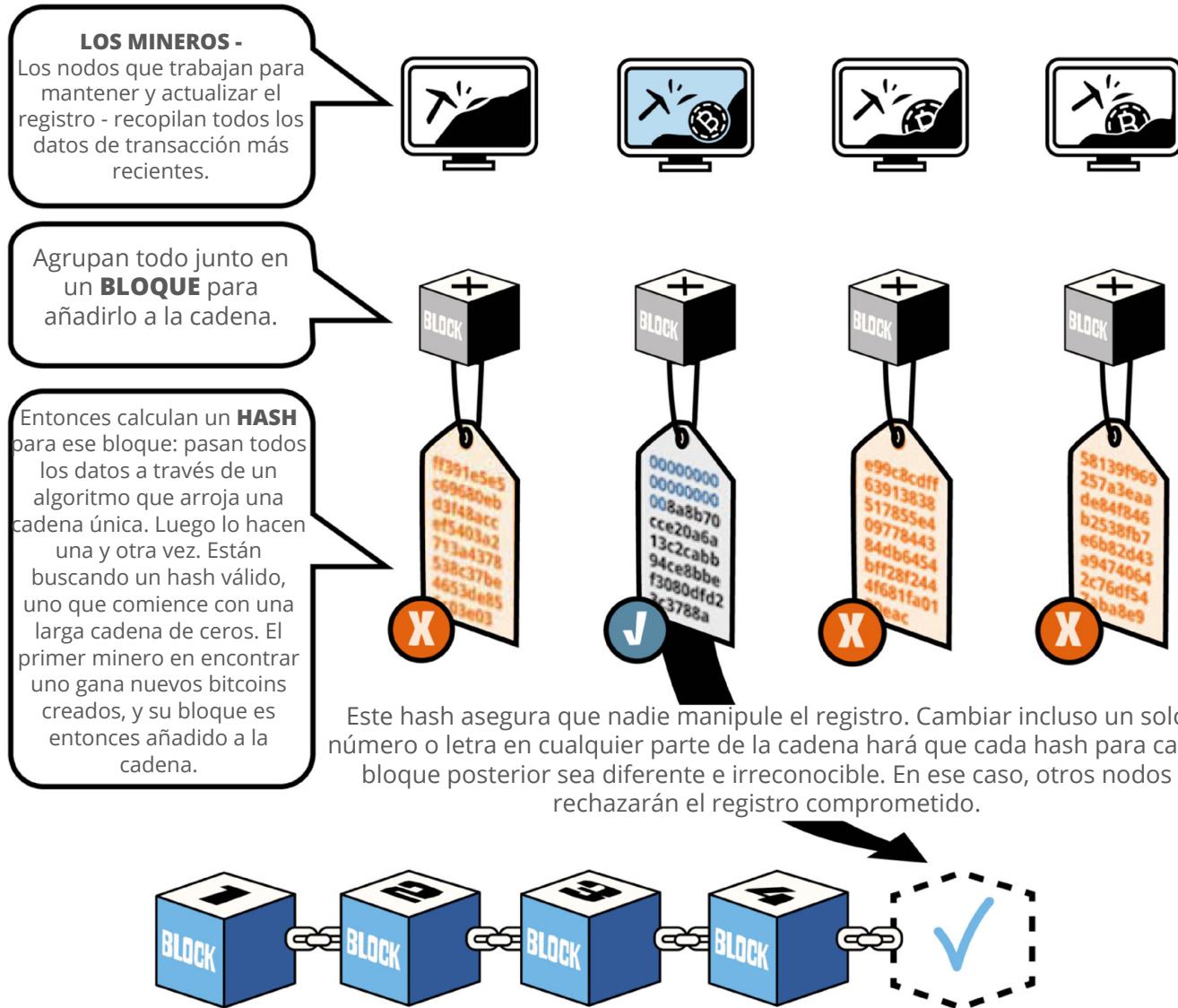
- 1 Agrupar transacciones en bloques:**
Mientras los nodos verifican transacciones recién creadas que están esperando en el "mempool", los mineros seleccionan un subconjunto de estas para incluir en su bloque candidato.
- 2 Prueba de Trabajo:**
Los mineros compiten entre sí para encontrar el hash de bloque válido.
- 3 Difundir bloques válidos:**
Después de encontrar el hash de bloque válido, propagan el nuevo bloque a la red.
- 4 Obtener recompensas:**
Por último, reciben bitcoins recién creados y tarifas de transacción por agregar con éxito el bloque al blockchain.



Varios mineros pueden trabajar simultáneamente en la creación de nuevos bloques. El primer minero que descubre un hash de bloque que cumple con el objetivo establecido por la red lo anuncia a la red, y luego los demás mineros verifican las transacciones en el bloque candidato de ese minero para asegurarse de que sean válidas. Si las transacciones son realmente válidas, el bloque se agrega a la cadena de bloques. Los otros bloques creados por los demás mineros en ese momento no se añaden y se descartan. Este proceso ayuda a mantener el consenso dentro de la red y evita el doble gasto.

Un bloque candidato es un conjunto de transacciones que se están considerando para su adición a la cadena de bloques pero aún no se ha añadido





9.4 ¿Qué es el Mempool?

El "mempool" o piscina de memoria es como una sala de espera para las transacciones en la Red de Bitcoin. Cuando realizas una transacción, primero se transmite al Mempool antes de ser verificada, seleccionada y agregada a la cadena de bloques.

Imagina que estás esperando en la fila de un restaurante. Tu nombre se agrega a una lista de personas esperando una mesa. Cuando hay una mesa disponible, el anfitrión llama tu nombre y te sienta. De manera similar, una transacción de bitcoin se agrega al Mempool cuando se realiza, y se confirma y se agrega a la cadena de bloques cuando un minero la incluye en un bloque.

Una Introducción al Aspecto Técnico de Bitcoin

La mempool es donde las transacciones esperan a ser confirmadas en un bloque.

tx hsh 6053b699...
fee rate: 3 sat/vB

tx hsh bb3b8clfc...
fee rate: 1 sat/vB

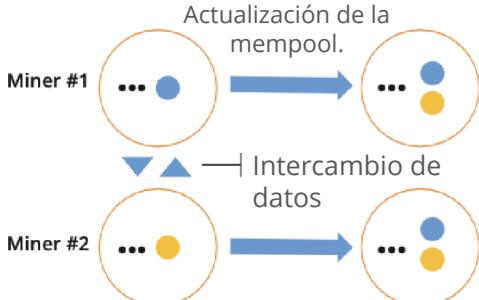
tx hsh d7c2532a9...
fee rate: 15 sat/vB

tx hsh 0ecdd9c6...
fee rate: 2 sat/vB



Cuando un nodo recibe una transacción por primera vez de un par, tiene que verificar que la transacción sea legítima. Nadie quiere transacciones defectuosas

La sincronización del mempool permite a los nodos compartir sus transacciones con otros nodos enviando un mensaje que contiene una lista de transacciones verificadas



El propósito principal de un mempool es:

- 1 Retransmitir transacciones no confirmadas.
- 2 Proporcionar transacciones a los mineros

Aceptar en Memory Pool (ATMP) implica verificar cosas como:

- ¿Ya tengo esta transacción?
- ¿Existe un conflicto con una transacción diferente en el mempool?
- ¿Los Bitcoin en cubren los Bitcoin fuera? ¿Las firmas prueban que las salidas anteriores pueden ser gastadas?
- ¿Hay suficientes tarifas?

¿Cómo se verifican y añaden las transacciones al Mempool?

Cuando las nuevas transacciones se transmiten a la red de Bitcoin, los nodos verifican estas transacciones para asegurarse de que sean válidas y de que los fondos no se hayan gastado antes. Una vez verificadas, los nodos las agregarán a su mempool. Luego, los nodos compartirán las transacciones con otros nodos para una verificación adicional. Finalmente, si la mayoría de los nodos están de acuerdo, las transacciones estarán disponibles para que los mineros las seleccionen e incluyan en un bloque. Sin embargo, hay varias razones por las cuales una transacción podría no confirmarse después de 72 horas:



Capítulo #9

1

Tarifas de transacción bajas:

Las transacciones con tarifas bajas pueden no procesarse lo suficientemente rápido, ya que los mineros son más propensos a elegir transacciones con tarifas más altas para incluirlas en sus bloques.

2

Congestión de la red:

Si la red está congestionada, puede haber un retraso en la confirmación de transacciones, incluso si tienen una tarifa alta.

3

Intento de doble gasto:

Si un actor malicioso intenta realizar un doble gasto, su transacción puede ser rechazada por la red.

4

Datos incorrectos o incompletos:

Si una transacción contiene datos incorrectos o incompletos, puede ser rechazada por la red.

5

Transacción malformada:

Si una transacción está malformada, puede ser rechazada por la red.

Para evitar que las transacciones sean rechazadas, se recomienda incluir una tarifa lo suficientemente alta para garantizar que la transacción se procese de manera oportuna y verificar que todos los datos en la transacción sean correctos antes de enviarla.

Actividad: Mempool

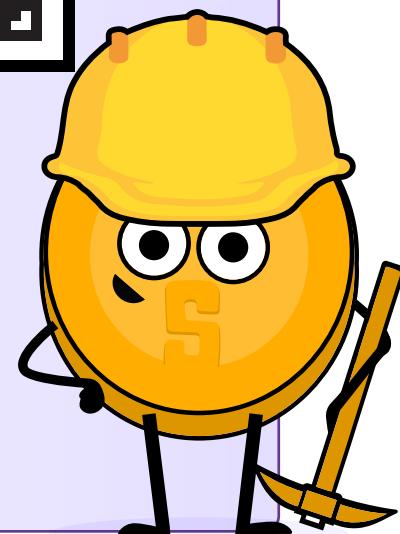
1

Escanee el siguiente QR code:

2

Revise los diversos elementos mostrados en la página, incluyendo los últimos bloques, transacciones confirmadas, el número de transacciones, el uso de memoria y el valor aproximado de todo el bloque. Responda las preguntas:

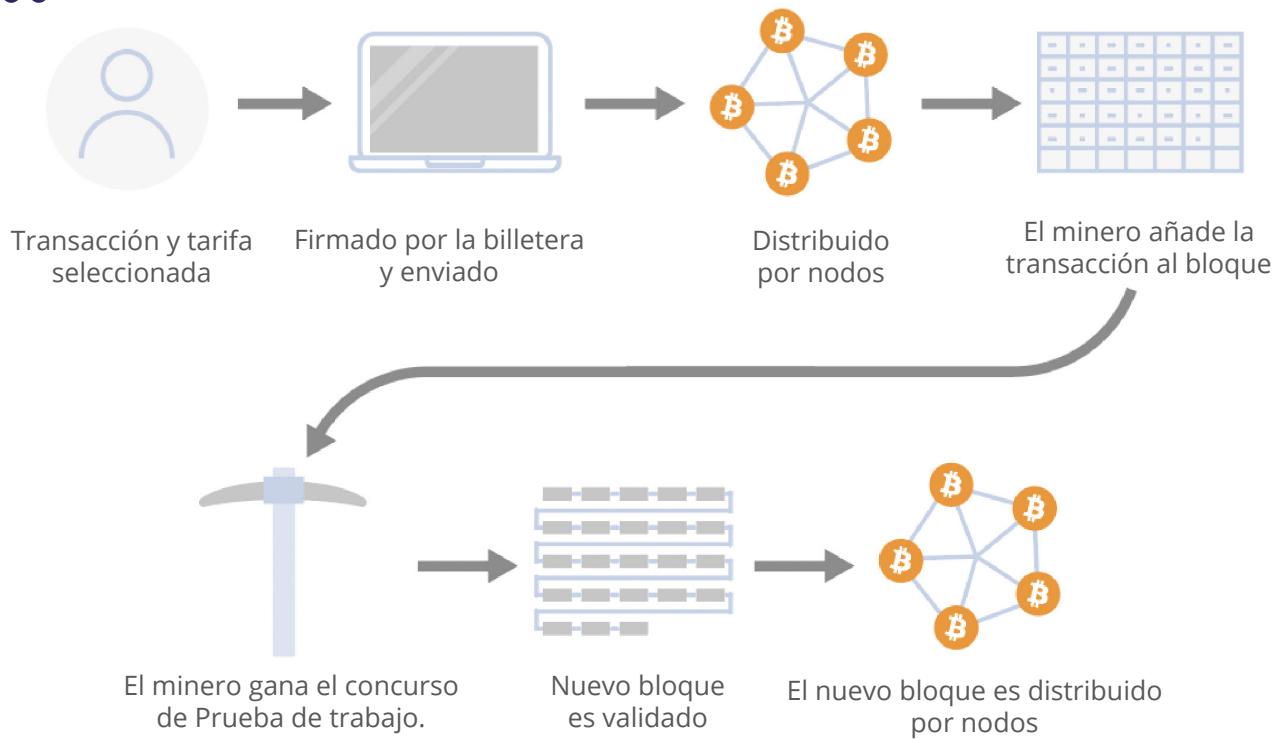
- 💡 ¿Cuál fue el último bloque minado?
- 💡 ¿Cuántas transacciones se incluyeron en ese bloque?
- 💡 ¿Cuál es el valor total negociado en bitcoin?
- 💡 ¿Cuál fue el tamaño en megabytes del bloque?
- 💡 ¿Con cuántos ceros comienza el nonce del bloque?
- 💡 ¿Cuánto bitcoin ganó el minero en total?
- 💡 ¿Cuál fue el valor total de las tarifas recibidas por el minero por agregar las transacciones a la red?
- 💡 Elija una de las transacciones de mayor valor en el bloque.
¿A cuántas direcciones de bitcoin se distribuyó la cantidad?



Una Introducción al Aspecto Técnico de Bitcoin

9.5 Cómo funcionan las transacciones de bitcoin de principio a fin

- 1** Adam quiere enviar bitcoin a Gerardo. Elige uno de sus UTXOs, crea una transacción y agrega todos los detalles necesarios, incluyendo la cantidad de bitcoin que quiere enviar, la dirección de recepción de Gerardo y una cantidad de tarifas de transacción superior al promedio.
- 2** Después de realizar una última verificación si todos los detalles son correctos, Adam utiliza su clave privada para firmar la transacción.
- 3** Adam transmite la transacción a la red de Bitcoin.



Desde: Stevenot, Ted, "What is a bitcoin node and how does one work?". Unchained Capital, 17 de enero de 2023, <https://unchained.com/blog/what-is-a-bitcoin-node/>

- 4** Los nodos en la red reciben la transacción y verifican su validez según las reglas de consenso (como verificar si la firma de Adam es válida y si tiene fondos suficientes para realizar la transacción).
- 5** La transacción se marca como válida y los nodos la propagan a otros nodos en la red, agregándola al mempool.
- 6** Dado que Adam eligió una tarifa de transacción lo suficientemente alta, casi todos los mineros incluyen su transacción en sus bloques.



Capítulo #9

7

Prueba de trabajo: Los mineros compiten y tratan de minar su bloque encontrando el hash de bloque válido. Uno de los mineros encuentra el hash y transmite su bloque a la red.

8

Los nodos reciben el bloque recién minado y verifican su validez. Esto incluye validar todas las transacciones dentro del bloque y asegurarse de que se cumpla el requisito de Prueba de Trabajo.

9

La mayoría de los nodos están de acuerdo en que el bloque es válido y lo agregan a la cadena de bloques. Gerardo recibe el bitcoin confirmado en su dirección de recepción.

10

A medida que se añaden bloques adicionales a la cadena de bloques en la hora siguiente, el número de confirmaciones para la transacción aumenta. A medida que aumenta el número de confirmaciones para la transacción, Gerardo adquiere mayor confianza en su éxito y naturaleza irreversible.



En resumen, el remitente firma la transacción con su clave privada, los nodos verifican los UTXOs de la transacción, y los mineros añaden la transacción verificada a la cadena de bloques. El receptor puede luego acceder al bitcoin utilizando su clave privada. Una vez que se mina un bloque, todas las transacciones incluidas en él se consideran confirmadas, y los UTXOs utilizados como entradas en estas transacciones se consideran gastados y no se utilizarán nuevamente.

Al concluir este capítulo, has obtenido valiosas ideas sobre los conceptos fundamentales de cómo funciona Bitcoin. Hemos cubierto aspectos esenciales, desde los fundamentos del dinero hasta el lado técnico de la tecnología Bitcoin. Ahora, unamos todo en el próximo capítulo. El Capítulo 10 espera, donde profundizaremos en la pregunta significativa: "¿Por qué Bitcoin?".

Capítulo #10

¿Por qué Bitcoin?

10.0 Introducción

Actividad - ¿Cómo podría ser el futuro con Bitcoin?

10.1 ¿Qué son las Monedas Digitales de Banco Central

(CBDC) y quién las controla?

10.2 La Filosofía de Bitcoin

Actividad: Discusión en clase — ¿Tienes derecho a controlar tu propio dinero?

10.3 Los Beneficios de Bitcoin

10.4 Un Futuro Empoderado

Actividad: Discusión en clase — ¿Cómo cambió tu perspectiva?

Libro de Trabajo Para Estudiantes

Versión en Español | 2025

¿Por qué Bitcoin?

Bitcoin es más que una moneda; es una revolución que devuelve el poder a la gente, ofreciendo un sabor de paz y libertad en un mundo hambriento de empoderamiento.

Mi Primer Bitcoin

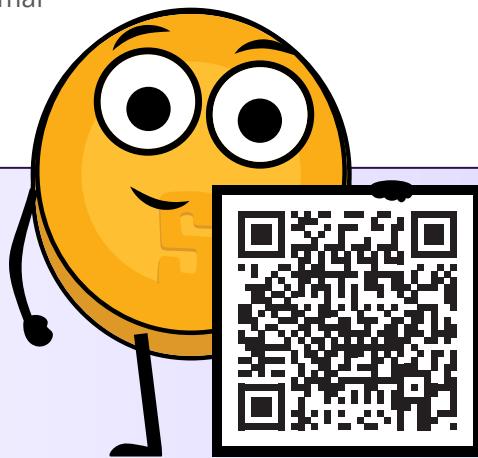
En este capítulo de conclusión, resumiremos las lecciones aprendidas a lo largo de nuestro viaje, haremos y discutiremos algunas preguntas importantes y exploraremos el futuro de Bitcoin.

Bitcoin no es solo una tecnología, es un tipo de red que impulsa una nueva forma de dinero cuyo suministro no puede ser cambiado por ninguna parte individual. La humanidad nunca ha tenido una forma de dinero con un suministro fijo y sin control centralizado. Si es ampliamente adoptado, Bitcoin es una herramienta que desbloquea un movimiento para un cambio positivo que puede transformar las vidas de las personas en todo el mundo. Representa una revolución pacífica hacia la libertad y equidad colectivas, abriendo nuevas oportunidades para la humanidad mediante la creación de un sistema monetario global compartido.

Como un sistema global descentralizado, Bitcoin permite una mayor libertad financiera, transfiriendo poder de unos pocos a muchos. Proporciona una plataforma segura y resistente a la censura para almacenar y transferir valor, empoderando a las personas para tomar el control de su riqueza y proteger su poder adquisitivo. Esto es especialmente importante en el clima económico incierto de hoy, donde el sistema financiero tradicional enfrenta desafíos sin precedentes.

Actividad: Ver el video

Las posibilidades de cambio positivo son inmensas, por eso te invitamos a ver este video para conocer más.



A continuación, veremos otra forma de moneda digital llamada Moneda Digital de Banco Central (CBDC) y evaluaremos cómo son similares y diferentes a Bitcoin.

10.1 ¿Qué son las Monedas Digitales de Banco Central (CBDC) y quién las controla?

Las Monedas Digitales de Banco Central, o CBDC, son versiones digitales de dinero fiduciario regular. Las CBDC siguen las mismas reglas que el dinero fiduciario regular, donde una autoridad central, como el gobierno, puede crear más suministro y, por lo tanto, es capaz de reducir el poder adquisitivo de las personas. Sin embargo, las CBDC también otorgan a los gobiernos herramientas nuevas y potentes para controlar cómo se utiliza ese dinero por parte de las personas en todo el mundo.

Según la investigación de la Fundación para los Derechos Humanos (HRF), 119 de 193 gobiernos en todo el mundo están investigando, probando o utilizando CBDC.

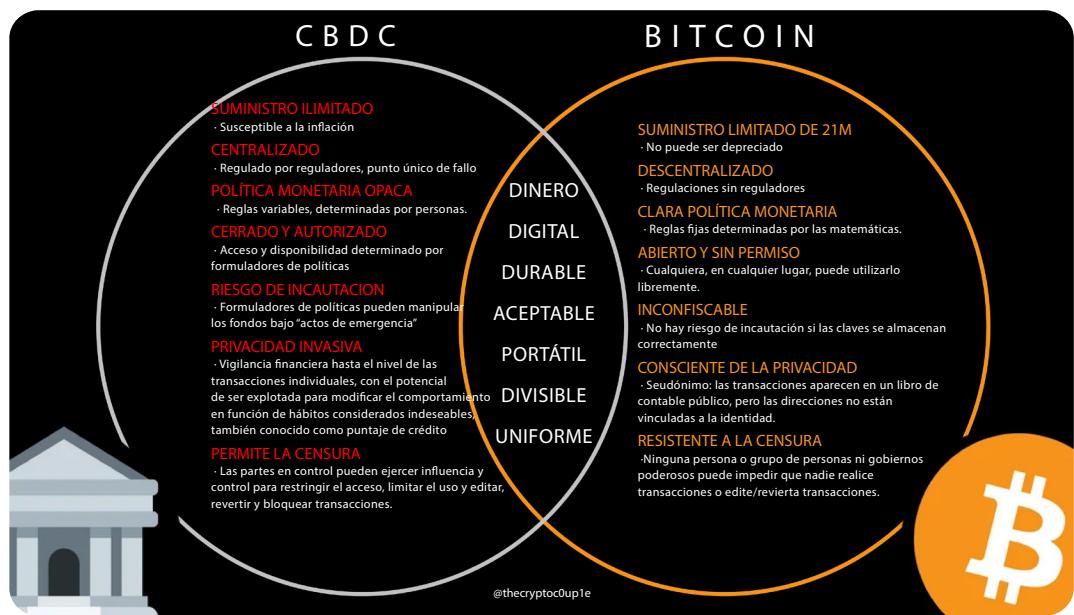
Puedes verificar si tu país está intentando implementar CBDCs en el rastreador de CBDC de la Fundación para los Derechos Humanos en
<https://cbdctracker.hrf.org/home> or
<https://cbdctracker.org/>



Entonces, ¿qué hace que las CBDC sean diferentes del dinero fiduciario regular además de ser digitales? Es crucial entender, que a diferencia del dinero fiduciario regular en forma de papel o monedas, las CBDC permiten al gobierno observar y controlar digitalmente cada transacción a nivel mundial. Esto significa que el gobierno puede detener ciertas transacciones o incluso congelar toda tu cuenta si no les gusta a quién envías dinero o cómo estás usando tu dinero.

Por ejemplo, imagina que quieres enviar dinero a un familiar en un país que necesita ayuda, pero tu gobierno local rechaza tu transacción porque no están de acuerdo con los líderes de ese país. O imagina ir a la tienda a comprar algo que te gusta, pero no puedes porque expresaste tu opinión en las redes sociales. Las CBDC otorgan a los gobiernos un poder ilimitado para controlar cómo se usa el dinero en todo el mundo, limitando la capacidad de las personas para gastar dinero según sus propias elecciones.

Algunos incluso argumentan que las CBDC permitirían a los gobiernos poderosos hacer cumplir políticas tiránicas a nivel global, con solo presionar un interruptor, sin necesidad de agentes de aplicación humanos. Tanto las CBDC como Bitcoin son digitales, pero más allá de esta similitud, representan formas muy diferentes de dinero con filosofías distintas, lo que conduce a resultados variados para la humanidad.



¿Por qué Bitcoin?

10.2 La Filosofía de Bitcoin

En los capítulos 6 y 9, descubrimos que las personas que ejecutan un Nodo ayudan a mantener seguras las reglas de Bitcoin. Esto es importante porque, por primera vez en la historia, personas como nosotros podemos ser parte de un equipo que se asegura de que las reglas de nuestro sistema monetario estén protegidas. Estas reglas incluyen el hecho de que solo hay una cantidad limitada de dinero y que ninguna parte individual puede cambiar estas reglas. Es una oportunidad especial para que las personas comunes ayuden a mantener seguro y confiable nuestro dinero.

La filosofía de Bitcoin se trata de empoderamiento, libertad, independencia financiera, pensamiento crítico y el concepto de que todos deberíamos tener voz en las reglas del sistema que elegimos para nosotros mismos. A diferencia del sistema fiduciario controlado por poderosas partes centrales, Bitcoin funciona en una red donde ninguna parte individual tiene todo el control. Esto significa que, a diferencia de otros tipos de dinero, como las CBDC, nadie puede quitarte tu propiedad o impedirte gastar tu dinero como quieras.

En el mundo fiduciario, tener más riqueza se traduce directamente en tener más influencia y control. Contrariamente, Bitcoin opera de una manera que se trata de dar poder a la gente. Es un esfuerzo de equipo donde todos, independientemente de cuánto dinero tengan, juegan un papel crucial en el sistema. Imagínalo como una fuerza colectiva, donde tu tamaño financiero no significa automáticamente que lo controles todo. Bitcoin está construido sobre reglas inalterables y, en esta armonía, es como si la humanidad misma estuviera controlando el sistema. No son unos pocos grandes tomadores de decisiones; somos todos trabajando juntos, al igual que una comunidad resiliente, guiando el curso de Bitcoin sin que ninguna autoridad única le diga qué hacer.

Mientras que en el sistema fiduciario los poderosos dictan las reglas, en el ecosistema Bitcoin, es la fuerza colectiva de individuos la que sostiene la red. Ninguna entidad única, independientemente de la riqueza, puede dictar el camino del ecosistema Bitcoin. Es una inversión de la dinámica de poder tradicional, donde la resiliencia del sistema no está en manos de unos pocos, sino en el poder colectivo de cada participante.

La idea principal es crear un sistema seguro, claro y justo donde todos puedan acceder al dinero global de manera equitativa.

Actividad: Discusión en clase — ¿Tienes derecho a controlar tu propio dinero?

- 1 ¿Es el dinero una necesidad humana y un derecho humano? ¿Y por qué?
- 2 Si no puedes gastar tu dinero como quieras, enviarlo a quien quieras o llevar tu dinero contigo a un nuevo país, ¿realmente es tuyo? ¿Y por qué?
- 3 ¿Por qué dejó de usarse el trueque? ¿Cuál es el problema con la doble coincidencia de deseos?
- 4 ¿Qué evento histórico fue el más impactante para ti? ¿Por qué es importante entender el shock de Nixon y su relevancia para todos hoy?
- 5 ¿Cómo es diferente el dinero con un suministro fijo de las monedas fiduciarias tradicionales?



Capítulo #10

- 6 ¿Cuándo se creó Bitcoin, por quién, con qué propósito y cómo define este propósito el concepto de un sistema descentralizado?
- 7 ¿Cuál es la diferencia entre una billetera custodial y una billetera no custodial? ¿Cuál fue tu billetera favorita?
- 8 ¿Qué entiendes sobre la Red Lightning? ¿Qué tipo de transacciones usarías en ella?
- 9 ¿Por qué ejecutar tu propio nodo apoya a la red?
- 10 ¿Cómo te empodera tener control sobre tu propio dinero en tu vida diaria y en la planificación futura?
- 11 ¿De qué manera puede la libertad financiera mejorar tu capacidad para contribuir positivamente a tu comunidad o sociedad?

10.3 Los Beneficios de Bitcoin

"Hyperbitcoinization" es un futuro teórico donde Bitcoin se convierte en el sistema monetario global dominante. Esto significaría que Bitcoin sería utilizado por todos, en todas partes y para todo, desde comprar café hasta pagar facturas e incluso comprar una casa.

El creciente interés en Bitcoin por parte de individuos, empresas, países y gobiernos destaca el impacto potencial de su adopción generalizada en la economía y la sociedad. Aquí hay algunos de los beneficios de un mundo hiper-bitcoinizado:

- 1 **Un futuro de autosoberanía:**
Un futuro de autodeterminación es aquel en el que las personas de todo el mundo tienen control total sobre su propia identidad y activos digitales. Esto podría conducir a una mayor inclusión financiera, libertad, privacidad, seguridad y, por lo tanto, contribuir a un mayor florecimiento humano, abundancia y felicidad general.
- 2 **Un almacenamiento confiable de valor:**
La escasez digital de Bitcoin lo convierte en un almacenamiento confiable de valor, lo que podría animar a más personas a usarlo como medio de ahorro para el futuro.
- 3 **Cambios en la política monetaria:**
Si Bitcoin llegara a ser ampliamente adoptado, podría deshacer la capacidad de los gobiernos de controlar la oferta de dinero a través de herramientas tradicionales de política monetaria. La adopción masiva de Bitcoin potencialmente aumentaría el poder adquisitivo de las personas y alentaría a la sociedad a moverse hacia actividades de baja preferencia temporal.
- 4 **Mayor transparencia y trazabilidad:**
El registro inmutable y a prueba de manipulaciones de todas las transacciones en la cadena de bloques podría aumentar la transparencia y la responsabilidad en diversas industrias y sectores. Actualmente, las entidades poderosas tienen la capacidad de mover billones de dólares en todo el mundo sin una visibilidad clara sobre dónde van estos fondos o cómo se utilizan. Al proporcionar un registro abierto y verificable de transacciones financieras, Bitcoin podría garantizar que el movimiento de capital se vuelva más responsable y accesible para el público.

¿Por qué Bitcoin?

5

Una revolución en el mercado de remesas:

El mercado de remesas implica la transferencia de fondos de una parte a otra, a menudo a través de fronteras internacionales. A pesar de los costos decrecientes, las remesas siguen siendo relativamente costosas en comparación con las transferencias bancarias nacionales, especialmente para cantidades pequeñas. La Red Lightning ofrece transacciones rápidas y de bajo costo, lo que la hace adecuada para el mercado de remesas y aborda los altos costos y otros desafíos asociados con las remesas, como los tiempos lentos de liquidación y las restricciones en el horario comercial.

6

Energía abundante:

Cuando hay mucha energía asequible, las sociedades prosperan y muchas industrias y comunidades pueden satisfacer la creciente necesidad de energía en hogares, empresas y nuevas tecnologías. La minería de Bitcoin incentiva a los mineros a utilizar energía excedente que normalmente se desperdiciaría de fuentes de energía sostenible como la solar, eólica e hidroeléctrica. Los mineros de Bitcoin utilizan esta energía excedente para crear nuevos bitcoins a través de actividades mineras, asegurar la red y ofrecer la energía excedente que generan de vuelta a la red eléctrica que la sociedad utiliza cuando es necesario.

10.4 Un Futuro Empoderado

Bitcoin es dinero.

El dinero ayuda a las personas a comunicar qué actividades, bienes y servicios son más importantes dentro de la sociedad. Como hemos visto en este curso, cuando el dinero está controlado por autoridades centralizadas, será manipulado.

Uno de los errores que la humanidad sigue repitiendo a lo largo de la historia es manipular el dinero, lo que luego afecta negativamente a individuos, familias, empresas, gobiernos y, en última instancia, a la prosperidad humana global.

Al sacar el control del dinero de las manos de partes centralizadas y, en cambio, utilizar dinero con un suministro fijo que ninguna parte individual puede cambiar, creamos un mundo diferente. Uno donde no tenemos que confiar en que el hombre haga lo correcto, sino más bien uno en el que el hombre no puede hacer lo incorrecto.

Este es un mundo fundamentalmente diferente.

Y tú, querido estudiante, puedes ser parte de la creación de este mundo. Usando Bitcoin, ejecutando tu propio nodo y ayudando a tu próximo a aprender más sobre el futuro del dinero, tú estás votando por un mundo diferente.

Actividad: Discusión Final en Clase — ¿Cómo cambió tu perspectiva?

Por favor, responde las 5 preguntas a continuación:



Capítulo #10

¿Por qué necesitamos dinero?

¿Qué es el dinero?

¿Por qué Bitcoin?

¿Quién controla el dinero?

¿Qué le otorga "valor" al dinero?



Capítulo #10

¿Qué pregunta tienes sobre el dinero? Escribe tu pregunta aquí para compartirla con la clase.

- 1** Regresa a la primera actividad del capítulo 1 y compara tus nuevas respuestas con tus respuestas anteriores.
- 2** Compara y discute las respuestas y preguntas originales. ¿Algo cambió?
- 3** Hazte esta pregunta final: ¿Cuál es mi próximo paso? ¿Y cómo puedo usar este nuevo conocimiento para empoderarme?



Si estás listo para dar el siguiente paso, revisa los recursos adicionales en la siguiente sección, donde hemos seleccionado los mejores recursos para mayor aprendizaje y éxito.

Recursos Adicionales

1. ¿Por qué usar bitcoin?

a) 'El Caso Alcista de Bitcoin' por Vijay Boyapati:

Este artículo presenta el argumento de por qué bitcoin es un activo valioso y por qué tiene el potencial de convertirse en una moneda global dominante. El autor cubre los aspectos técnicos y económicos de bitcoin que lo convierten en una sólida oportunidad de inversión.

b) 'Por Qué Importa Bitcoin' por Aleks Svetski (1 hora):

Este video aborda la importancia de bitcoin como un activo digital descentralizado y cómo puede impactar el sistema financiero actual. El orador explora el potencial de bitcoin para llevar la libertad financiera a personas de todo el mundo.

c) 'Por Qué Bitcoin' por Wiz:

Este artículo proporciona una visión general de los beneficios de usar bitcoin como moneda y reserva de valor. Destaca la naturaleza descentralizada de bitcoin y cómo permite una mayor libertad financiera y seguridad.

2. ¿Qué es Bitcoin?

a) 'Cómo Funciona Bitcoin Bajo el Capó' por Curious Inventor:

<https://www.youtube.com/watch?v=Lx9zgZCMqXE> Este video proporciona una explicación detallada de los aspectos técnicos de bitcoin y cómo funciona.

b) '¿Qué Es Bitcoin?' por Greg Walker:

Este artículo proporciona una explicación exhaustiva de qué es bitcoin, incluyendo su historia, tecnología y cómo difiere de las monedas tradicionales.

c) 'Bitcoin — El Génesis' por RT (30 minutos):

Este video cubre la creación y los primeros días de bitcoin. Explora las motivaciones del misterioso creador, Satoshi Nakamoto, y cómo evolucionó el concepto de bitcoin.

3. Aprendizaje Adicional:

a) 'El Estándar Bitcoin' (1 hora 40 minutos):

Este audiolibro explora el contexto económico e histórico que llevó a la creación de bitcoin. Cubre los beneficios de una moneda descentralizada y el potencial de bitcoin para convertirse en un estándar global.

c) "Bitcoin Babies"

por Naomi Wambui - <https://bitcoinnbabies.com/>
Twitter: [@btcbabies](#) - [@ngachanaomi1](#)

Un recurso en pdf gratuito para empoderar a las madres en países del tercer mundo.

b) "Introducción al Pensamiento Austríaco de Bitcoin" (1 hora):

Esta conferencia de audio cubre la Escuela Austriaca de economía y cómo se relaciona con el concepto de bitcoin. Proporciona una mirada profunda a los principios económicos detrás de bitcoin y cómo se alinea con el pensamiento austriaco.

d) BTC Sessions

Un canal educativo de YouTube exclusivo para bitcoin con tutoriales y guías útiles - <https://www.youtube.com/@BTCSessions>

4. Cursos:

a) Summer of Bitcoin

<https://www.summerofbitcoin.org/>: un programa global de pasantías de verano en línea centrado en introducir a los estudiantes universitarios al desarrollo y diseño de código abierto de bitcoin



b Chaincode Labs

<https://learning.chaincode.com/#FOSS>: cursos en línea y un programa de residencia que permite a los estudiantes aprender las habilidades necesarias para trabajar en el desarrollo del protocolo Bitcoin.

5. Autores Importantes

- a Alex Gladstein: *'Verifica tu Privilegio Financiero'*
- b Alex Swan: *'Terapia de Encuentro Anclada: Perspectivas, Características y Aplicaciones'*
- c Amanda Cavalieri: *'Bitcoin y el Sueño Americano: La Nueva Tecnología Monetaria que Trasciende Nuestra División Política'*
- d Anita Posch: *'Aprende Bitcoin: Conviértete en Soberano Financiero'*
- e Eric Yakes: *'La 7^a Propiedad: Bitcoin y la Revolución Monetaria'*

c Saylor Academy

Educación gratuita en múltiples disciplinas:
<https://www.saylor.org/>

- f Jeff Booth: *'El Precio del Mañana: Por qué la Deflación es la Clave para un Futuro Abundante'*
- g Jimmy Song: *'El Pequeño Libro de Bitcoin: Por qué Bitcoin Importa para tu Libertad, Finanzas y Futuro'*
- h Nik Bhatia: *'Dinero en Capas: Desde el Oro y los Dólares hasta Bitcoin y las Monedas Digitales de los Bancos Centrales'*
- i Robert Breedlove: *'Gracias a Dios por Bitcoin: La Creación, Corrupción y Redención del Dinero'*
- j Lyn Alden: *'Dinero Roto'*

6. Autores Citados

a Curious Inventor:

<https://www.youtube.com/@CuriousInventor>

b Anil Patel:

Twitter: [@anilsaidso](https://twitter.com/anilsaidso)

7. Otros Recursos:

- 1 **Bitcoin.org:** El sitio web oficial del protocolo Bitcoin
- 2 **Btcointalk.org:** Btcointalk es un foro donde los usuarios pueden discutir temas relacionados con Bitcoin, hacer preguntas y compartir información. Es un gran lugar para aprender de otros entusiastas y expertos en Bitcoin.
- 3 **Bitcoincore.org:** Este es el software original de Bitcoin y todavía es ampliamente utilizado por muchos usuarios y desarrolladores. Proporciona un conjunto poderoso de herramientas para interactuar con la red Bitcoin y construir aplicaciones de Bitcoin.
- 4 **Bitcoinwiki.org:** Este es un recurso impulsado por la comunidad que proporciona una guía completa sobre todo lo relacionado con Bitcoin. Cubre desde los aspectos técnicos de Bitcoin hasta su historia y casos de uso.
- 5 **Bitcoinmagazine.com:** Esta es una publicación en línea que cubre noticias e ideas relacionadas con Bitcoin y otras criptomonedas. Proporciona una excelente manera de mantenerse al día con los últimos desarrollos en el ecosistema Bitcoin.
- 6 **Bitcoin.Design:** Un repositorio de diseño relacionado con bitcoin de código abierto para ilustraciones, sitios web, plantillas e iconos.
- 14 **Yzer:** <https://yzer.io/> Educación sobre Bitcoin sencilla y móvil. Aprenda sobre Bitcoin, finanzas, economía y gane Sats.

- 7 **NOSTR:** <https://nostr.com/> - redes sociales donde realmente eres dueño de tus datos.
- 8 **Simple X:** <https://simplex.chat/> - un protocolo de aplicación privada y descentralizada.
- 9 **Configurar un Nodo Bitcoin:** Raspberry Pi DIY por Keith Muka:
https://github.com/kdmukai/raspberrypi_bitcoin_node_tutorial?tab=readme-ov-file
- 10 **Cómo seleccionar una billetera de bitcoin:**
<https://bitcoin.org/en/choose-your-wallet> - utiliza tus conocimientos recién adquiridos para seleccionar la billetera adecuada para ti.
- 11 **BitcoinIcons.com:** - <https://bitcoinicons.com/> - Una colección de iconos de bitcoin gratuitos.
- 12 **Bitcoin Para Negocios Locales:**
<https://bitcoinfoforlocalbusiness.com/> - Un conjunto de volantes para ayudarte a compartir el valor de bitcoin con tus negocios locales favoritos.
- 13 **Mempool.Space:** <https://mempool.space/> - un proyecto de mempool de código abierto que también presenta datos y gráficos de la red Lightning.

Conceptos Clave por Capítulo

Capítulo 1:

-  **Introducción al Curso:**
Explora los objetivos del curso y las expectativas para el Diploma de Bitcoin.
-  **Actividad Reflexiva — Definición de Dinero:**
Participa en un ejercicio reflexivo proporcionando cinco respuestas a preguntas clave sobre el dinero.
-  **Discusión en Clase — Por qué necesitamos dinero:**
 - Participa en una discusión a nivel de clase explorando la necesidad fundamental del dinero.
 - Comparte y compara perspectivas individuales sobre la importancia del dinero.
 - Establece las bases para comprender el papel del dinero en los sistemas económicos.

Capítulo 2:

-  **Comprensión del Dinero:**
 - Explora la definición y concepto fundamentales del dinero.
 - Discute las diversas perspectivas dentro de la clase para comprender la naturaleza multifacética del dinero.
-  **Psicología del Dinero:**
 - Comprende los aspectos psicológicos del dinero, incluyendo la escasez, la preferencia temporal y las compensaciones.
 - Participa en la actividad "Preferencia Temporal" para relacionar elementos psicológicos con escenarios de la vida real.
-  **Funciones, Propiedades y Tipos:**
 - Adéntrate en las funciones, propiedades y tipos de dinero.
 - Reconoce la importancia de estos aspectos en la definición y utilización del dinero.

Capítulo 3:

-  **Introducción a la Historia y Evolución del Dinero:**
Explora la historia y evolución del dinero. Comprende cómo las formas antiguas de intercambio llevaron al desarrollo de la moneda que usamos hoy.
-  **Revolución de la Moneda Digital:**
 - Descubre el pináculo actual de la evolución del dinero: la moneda digital.
 - Comprende cómo existe solo en forma electrónica, permitiendo transacciones instantáneas y de bajo costo a nivel mundial.
 - Aprende sobre el papel significativo que desempeñó Bitcoin en resolver los desafíos iniciales de las monedas digitales, preparándolas para su uso en todo el mundo.
-  **Evolución de la Moneda:**
Explora la transición desde formas antiguas como conchas y cuentas hasta el surgimiento de la acuñación y el papel moneda. Sigue el viaje desde el papel hasta el plástico, desentrañando la evolución de la moneda a lo largo de la historia.
-  **Actividad del Juego de Trueque:**
Participa en una experiencia práctica de juego de trueque para entender los desafíos del intercambio directo y apreciar la necesidad de un sistema más eficiente.



Capítulo 4:



Orígenes del Dinero Fiat:

Explora los orígenes del dinero fiat a través de una breve descripción histórica, comprendiendo cómo se convirtió en una forma dominante de moneda.



Actividad de Banca de Reserva Fraccionaria:

Participa en la actividad de Banca de Reserva Fraccionaria para obtener información sobre cómo opera este sistema, destacando su dependencia de la deuda y las implicaciones para la economía en general.



El Sistema Fiat:

Comprende los aspectos fundamentales del sistema fiat, incluyendo su naturaleza como sistema monetario por decreto, el papel de la banca de reserva fraccionaria y los actores clave que controlan este sistema.

Capítulo 5:



Disminución del Poder Adquisitivo:

Comprende el concepto de inflación monetaria y su impacto en el poder adquisitivo. Participa en la Actividad de Efectos de la Inflación: Una Subasta para experimentar los efectos de primera mano.



Actividad de Consecuencias del Sistema Fiat:

Participa en la actividad de Consecuencias del Sistema Fiat, arrojando luz sobre las repercusiones más amplias del marco monetario actual.



Monedas Digitales del Banco Central (CBDCs):

Explora el panorama en evolución de las Monedas Digitales del Banco Central (CBDCs) y su impacto potencial en el futuro del dinero.



Carga Global de Deuda e Inequidad Social:

Explora los impactos duales de la carga global de deuda y la desigualdad social. Reconoce las consecuencias individuales y sociales, haciendo hincapié en la pérdida de poder adquisitivo y la ampliación de la brecha de riqueza.



Los Cypherpunks y la Descentralización:

Aprende la historia de los Cypherpunks y su motivación para buscar una moneda descentralizada. Diferencia entre sistemas centralizados y descentralizados, obteniendo información de una breve historia de las monedas digitales.

Capítulo 6:



Satoshi Nakamoto y la Creación de Bitcoin:

Explora la figura misteriosa de Satoshi Nakamoto y la historia de origen de Bitcoin, comprendiendo las motivaciones iniciales detrás de su desarrollo.



Actividad en Clase — Construcción de Consenso:

Participa en la actividad de Construcción de Consenso en una Red Peer-to-Peer para obtener ideas prácticas sobre cómo se logra el consenso dentro de la red Bitcoin.



Bitcoin como Dinero Digital Sólido:

Examina el papel de Bitcoin como dinero digital sólido, discutiendo su evolución, funciones, propiedades y participa en una discusión en clase sobre si Bitcoin califica como dinero sólido.



Cómo Funciona Bitcoin

Observa la mecánica de Bitcoin, incluyendo el Mecanismo de Consenso Nakamoto. Identifica a los actores clave en la red de Bitcoin, como mineros, nodos, usuarios, desarrolladores y proyectos, y comprende las dinámicas colaborativas entre ellos.



Bitcoin como Dinero Digital Sólido:

Examinar el papel de Bitcoin como dinero digital sólido, discutiendo su evolución, funciones y propiedades, y participa en una discusión de clase sobre si Bitcoin califica como dinero sólido.

Conceptos Clave por Capítulo

Capítulo 7:

Transacciones Peer-to-Peer:

Participa en transacciones descentralizadas para experimentar los principios fundamentales de los intercambios de Bitcoin

Configuración de una Billetera de Bitcoin:

Aprende los pasos esenciales para descargar, crear claves y hacer una copia de seguridad de una billetera de Bitcoin para transacciones seguras.

Ahorro e Investigación Independiente (DYOR):

Comprende el ahorro en Bitcoin como reserva de valor y la importancia de la investigación independiente para la toma de decisiones informada.

Capítulo 8:

Introducción a la Red Lightning:

Reconoce la evolución de Bitcoin a través de tecnologías como la Red Lightning, mejorando sus capacidades.

Configuración de una Billetera Lightning:

Aprende los pasos esenciales para configurar una billetera Lightning de Bitcoin, facilitando transacciones más rápidas y escalables.

Actividad Práctica:

Participa en una carrera práctica de relevos con billeteras Lightning, promoviendo una comprensión dinámica de las transacciones en la Red Lightning.

Capítulo 9:

El Libro Mayor de Bitcoin:

Comprende el concepto de un libro mayor descentralizado facilitado por nodos y mineros, garantizando transparencia y seguridad.

El Modelo UTXO:

Comprende el modelo de Salida de Transacción no Gastada (UTXO) como un aspecto fundamental del proceso de transacción de Bitcoin.

Claves Públicas y Privadas:

Explora la importancia de la seguridad criptográfica en las transacciones de Bitcoin a través de claves públicas y privadas, junto con una actividad que demuestra el hash SHA 256.

Tipos de Billetera de Bitcoin

Diferencia entre billeteras de código abierto, cerrado, custodiales y no custodiales, comprendiendo el papel de las claves en la seguridad

Adquisición de Bitcoin:

Explora métodos como transacciones peer-to-peer e intercambios, discutiendo preocupaciones de privacidad relacionadas con los procesos KYC.

Tipos de Billetera Lightning

Diferencia entre billeteras Lightning de código abierto, cerrado, custodiales y no custodiales para diversas preferencias de usuario.

Transacciones Lightning:

Explora el proceso de enviar y recibir transacciones Lightning, enfatizando la velocidad y eficiencia de la Red Lightning.

Nodos y Mineros de Bitcoin:

Investiga los roles de nodos y mineros en el mantenimiento de la red Bitcoin, cubriendo aspectos como emisión, escasez, reducción a la mitad y dificultad.

Cómo Funcionan las Transacciones de Bitcoin:

Obtén información sobre todo el ciclo de vida de una transacción de Bitcoin, involucrando al remitente, receptor, nodos, mineros y el mempool, con una actividad dedicada centrada en el mempool.

Capítulo 10:

Fundamentos Filosóficos de Bitcoin:

Explora la filosofía fundamental detrás de Bitcoin, comprendiendo cómo surgió como respuesta a desafíos económicos, con un enfoque en su impacto en la libertad financiera y cómo difiere de las monedas tradicionales.

Futuro de Bitcoin:

Profundiza en la trayectoria potencial y los desarrollos futuros de Bitcoin como una moneda digital revolucionaria.

Reflexión del Diploma:

-  Resume las lecciones clave del Diploma de Bitcoin, alentando a los estudiantes a reflexionar sobre su viaje y las ideas obtenidas.
-  Las actividades incluyen ver un video sobre "¿por qué Bitcoin?" y revisitar las preguntas del Capítulo 1 para evaluar el crecimiento personal en la comprensión.

Glosario

Ataque del 51%: Un tipo de ataque en una red blockchain en el que una sola entidad o grupo controla la mayoría del poder informático de la red, lo que les permite manipular transacciones y potencialmente interrumpir la red.

Temporada de Altcoins: Un período de tiempo en el que las criptomonedas alternativas experimentan aumentos significativos de precios, a menudo debido a un mayor interés y adopción por parte de los inversores.

Altcoins: Monedas digitales excluyendo Bitcoin.

Intercambio Atómico: Un intercambio entre pares de una criptomoneda por otra sin necesidad de un intercambio centralizado o intermediario.

Subasta: Un proceso mediante el cual se venden bienes o activos al postor más alto.

Trueque: El intercambio de bienes y servicios sin el uso de dinero.

Canasta de Bienes: Una colección de bienes o servicios utilizados para medir los cambios en el costo de vida.

Bitcoin: Una moneda/sistema digital que permite a las personas enviarse dinero entre sí sin usar un banco.

Explorador de Bloques: Una herramienta utilizada para ver y explorar la blockchain, permitiendo a los usuarios ver bloques individuales, transacciones y direcciones de monedero.

Recompensa por Bloque: La cantidad de nuevos bitcoins que se otorgan a los mineros por agregar un nuevo bloque a la blockchain.

Blockchain: Un registro público de todas las transacciones de bitcoin que han tenido lugar.

BTC: La unidad utilizada para bitcoins. Una moneda digital que puede utilizarse para hacer compras o ser intercambiada.

Control de Capitales: Restricciones sobre el movimiento de dinero a través de las fronteras.

Banco Central (Fed): Una institución de propiedad gubernamental que gestiona la política monetaria de un país.

Centralización: La concentración de poder o control en una sola entidad.

Sistema Centralizado: Un sistema en el que el poder o el control se concentra en una sola entidad.

Almacenamiento en Frío: Un método de almacenamiento de bitcoins fuera de línea, lejos del riesgo de hackers u otras amenazas en línea.

Dinero Mercancía: Objetos que tienen valor por sí mismos y se utilizan como medio de intercambio, como el oro o la plata.



Confirmación: El proceso de una transacción que es procesada por la red y es muy poco probable que sea revertida. Los "mineros" verifican la autenticidad de las transacciones con su hardware y software informático. Se recomienda esperar al menos seis confirmaciones para evitar el doble gasto.

Mecanismo de Consenso: Un método utilizado en la tecnología blockchain para validar transacciones y asegurar la integridad de la blockchain.

Intercambio de Criptomonedas: Una plataforma donde los usuarios pueden comprar, vender e intercambiar criptomonedas por otros activos como moneda fiduciaria o otras criptomonedas.

Monedero de Criptomonedas: Un programa de software que almacena claves privadas y permite a los usuarios enviar, recibir y gestionar su criptomoneda.

Criptografía: Una rama de las matemáticas que ayuda a crear sistemas seguros.

Devaluación: La reducción en el valor de una moneda, a menudo al reducir la cantidad de metal precioso en una moneda.

Deuda: Dinero que se debe a otra persona.

Descentralización: La distribución de poder y control a través de una red en lugar de tener una autoridad central.

Organización Autónoma Descentralizada (DAO): Una organización o red gobernada por contratos inteligentes y ejecutada en una blockchain sin una autoridad central o una estructura de gestión.

Finanzas Descentralizadas (DeFi): Un movimiento dentro de la industria de las criptomonedas para crear productos y servicios financieros descentralizados que operan en una blockchain.

Sistema Descentralizado: Un sistema en el que el poder o el control se distribuye entre múltiples entidades.

Activo Digital: Una representación digital de valor que puede ser intercambiada o utilizada como reserva de valor, como los bitcoins.

Libro Mayor Distribuido: Una base de datos que se extiende a través de una red de computadoras en lugar de estar almacenada en un lugar central.

Doble Coincidencia de Deseos: El fenómeno donde dos partes en una economía de trueque tienen lo que la otra parte quiere y quieren lo que la otra parte tiene.

Doble Gasto: Cuando una persona intenta enviar sus bitcoins a dos destinatarios diferentes al mismo tiempo.

Transacción de Polvo: Una transacción que envía una cantidad muy pequeña de bitcoins que son demasiado pequeños para ser económicamente viables.

Glosario

Tipo de Cambio: El valor de una moneda en relación con otra.

FOMO: Fear Of Missing Out, por sus siglas en inglés, quiere decir “miedo a perderse algo”, un término usado para describir la sensación de ansiedad o arrepentimiento de que uno pueda perder una oportunidad rentable en el mercado de criptomonedas.

FUD: Miedo, incertidumbre y duda, un término usado para describir rumores o información negativa que puede causar pánico o declive en el mercado.

PIB: Producto Interno Bruto, el valor total de bienes y servicios producidos en un país en un período de tiempo dado.

Hard Fork: Un cambio en el protocolo de Bitcoin que crea una nueva versión de la blockchain que no es compatible con la versión anterior (es decir, Bitcoin Cash).

Monedero de Hardware: Un dispositivo físico utilizado para almacenar claves privadas y gestionar criptomonedas, proporcionando seguridad mejorada sobre los monederos de software.

Función Hash: Una función matemática que toma datos de entrada de cualquier tamaño y produce una cadena de caracteres de tamaño fijo, comúnmente utilizada en criptografía y tecnología blockchain.

Tasa de Hash: Una forma de medir la potencia de procesamiento de la red Bitcoin.

HODL: Un término utilizado en la comunidad de criptomonedas para describir la retención de criptomonedas a largo plazo en lugar de venderlas o intercambiarlas.

Monedero Caliente: Un monedero de Bitcoin que está conectado a internet, lo que permite un fácil acceso a los bitcoins.

Importaciones: Bienes y servicios producidos en otro país y vendidos en el mercado nacional.

Inflación: Un aumento en el nivel general de precios de bienes y servicios en una economía.

Oferta Inicial de Moneda (ICO): Un método de recaudación de fondos en el que una nueva criptomoneda se vende a inversores a cambio de una criptomoneda más establecida, como Bitcoin.

Protocolo de Capa-1: La capa subyacente de una red blockchain que maneja los aspectos fundamentales de consenso, validación de transacciones y almacenamiento de datos.

Protocolo de Capa-2: Una capa secundaria construida sobre una red blockchain de capa-1, a menudo utilizada para mejorar la escalabilidad, velocidad y funcionalidad.

Libro Mayor: Un registro de transacciones financieras.

Red Lightning: Un protocolo de pago de capa-2 que permite transacciones de bitcoins más rápidas y más baratas utilizando canales fuera de la cadena para transacciones más pequeñas.



Medios de Intercambio: Objetos o sistemas ampliamente aceptados en intercambio por bienes y servicios.

Árbol de Merkle: Una estructura de datos similar a un árbol utilizada en la cadena de bloques de Bitcoin para verificar eficientemente la integridad de grandes conjuntos de datos.

Grupo de Minería: Un conjunto de mineros que trabajan juntos para aumentar sus posibilidades de encontrar nuevos bloques y ganar bitcoins.

Minería: El proceso de utilizar hardware de computadora para realizar cálculos matemáticos para la red Bitcoin para confirmar transacciones y aumentar la seguridad.

Política Monetaria y Fiscal: Las políticas de un banco central y gobierno, respectivamente, que influyen en la oferta de dinero y las tasas de interés en una economía.

Oferta Monetaria: La cantidad total de dinero en circulación en una economía.

Billetera Multifirma (Multisig): Una billetera que requiere múltiples firmas o aprobaciones antes de que una transacción pueda ser ejecutada, proporcionando seguridad y control adicionales.

Multifirma: Una característica de seguridad que requiere más de una clave privada para autorizar una transacción de bitcoin.

Red: Un grupo de entidades interconectadas.

Red de Nodos: Una red de computadoras o dispositivos conectados que respaldan y mantienen la red Bitcoin.

Nodo: Una computadora o dispositivo que está conectado a la red Bitcoin y participa en la verificación y transmisión de transacciones.

Token No Fungible (NFT): Un tipo de activo digital que representa un artículo único o irrepetible, frecuentemente utilizado para representar arte, colecciónables u otros objetos únicos.

Nonce: Un número aleatorio agregado a un encabezado de bloque para crear un hash que cumpla con el objetivo de dificultad.

Bloque Huérfano: Un bloque no incluido en la cadena principal de la cadena de bloques debido a ser invalidado por una cadena competitiva más larga.

Billetera de Papel: Una copia impresa de las claves privadas y públicas de un usuario utilizada para almacenar y gestionar criptomonedas fuera de línea.

P2P (Peer-to-Peer): Una red descentralizada en la cual los participantes interactúan directamente entre sí en lugar de a través de una autoridad central.

Glosario

Peg: Una tasa de cambio fija entre dos monedas donde una está fijada al valor de otra.

Blockchain Privada: Una blockchain controlada por una sola organización en lugar de ser descentralizada.

Clave Privada: Una pieza secreta de datos que demuestra el derecho de una persona a gastar bitcoins de una billetera específica a través de una firma criptográfica.

Prueba de Participación (PoS): Un mecanismo de consenso utilizado en algunas redes blockchain que requiere que los usuarios posean una cierta cantidad de criptomonedas para participar en la validación de transacciones.

Prueba de Trabajo: Un mecanismo de consenso que requiere que los usuarios realicen una cierta cantidad de trabajo computacional para participar en la red.

Cadena de bloques Pública: Una cadena de bloques abierta para que cualquiera pueda participar y verificar transacciones, haciéndola descentralizada.

Clave Pública: Un identificador único utilizado para recibir bitcoins derivados de la clave privada de un usuario a través de un proceso matemático.

Dirección Pública de Bitcoin: Una contraseña/número público utilizado para recibir bitcoins.

Libro Contable Público: Una base de datos descentralizada que mantiene un registro público de todas las transacciones en la red Bitcoin.

Poder Adquisitivo: La capacidad del dinero para comprar bienes y servicios.

Frase de Recuperación/Frase Semilla: Una serie de 12, 18 o 24 palabras que pueden usarse para generar múltiples pares de claves privadas y públicas. Estas pueden usarse para restaurar una billetera de Bitcoin.

Ratio de Reserva: La proporción de depósitos que un banco debe mantener como reservas.

Banca Restrictiva: Restricciones o limitaciones en los servicios bancarios o el acceso a los servicios bancarios.

Satoshi Nakamoto: El seudónimo utilizado por el creador (o creadores) anónimo(s) de Bitcoin.

Satoshi: La unidad más pequeña de Bitcoin, equivalente a 1/100,000,000 de un bitcoin. Está nombrado en honor al creador de Bitcoin, Satoshi Nakamoto.

Satoshis por Byte (sat/b): Una unidad utilizada para medir la cantidad de tarifa de transacción de bitcoin pagada por byte de datos de transacción.

SegWit (Testigo Segregado): Una actualización del protocolo Bitcoin que cambia la forma en que se almacenan los datos en la blockchain, permitiendo una mayor capacidad y tarifas de transacción más bajas.

Sidechain: Una blockchain conectada a otra blockchain, lo que permite la transferencia de activos o información entre las dos cadenas.

Firma: Un mecanismo matemático que permite a alguien probar la propiedad.

Contrato Inteligente: Un contrato autoejecutable con los términos del acuerdo escritos en código.

Soft Fork: Un cambio en el protocolo Bitcoin que es compatible con versiones anteriores del software.

Stablecoin: Un tipo de criptomoneda diseñada para mantener un valor estable, a menudo estando vinculada a una moneda fiduciaria u otro activo.

Oferta y Demanda: El principio económico de que el precio de bienes o servicios es determinado por la interacción entre la cantidad de bienes o servicios ofrecidos y la cantidad demandada.

Valor Temporal del Dinero: El principio de que el dinero vale más en el presente que en el futuro.

Token: Una unidad de valor creada en una blockchain, a menudo utilizada para representar un activo específico o utilidad dentro de un ecosistema particular.

Tokenización: El proceso de crear una representación digital de un activo o clase de activos en una blockchain, permitiendo la propiedad fraccionada y la transferibilidad.

Par de Comercio: Un conjunto de dos monedas o activos que pueden intercambiarse entre sí en un intercambio de criptomonedas.

Tarifa de Transacción: Una pequeña cantidad de bitcoins pagada por el remitente de una transacción, incentivando a los mineros a incluir la transacción en un bloque y agregarla a la blockchain.

ID de Transacción: Una cadena de números y letras que muestra los detalles de una transferencia de bitcoin (como la cantidad enviada, las direcciones del remitente y del destinatario, y la fecha de la transferencia) en la blockchain de Bitcoin.

Transacción: La transferencia de bitcoins de una dirección a otra en la red Bitcoin.

Sin Confianza: Un sistema o transacción que no requiere confianza en ningún tercero o intermediario, en lugar de ello, confiando en la seguridad y transparencia de la tecnología subyacente.

Glosario

Autenticación de Dos Factores (2FA): Una medida de seguridad que requiere dos métodos de autenticación, típicamente una contraseña y un código o dispositivo separado, para acceder a una cuenta o completar una transacción.

No Bancarizados: Individuos o comunidades sin acceso a servicios bancarios tradicionales.
Unidad de Cuenta: Una unidad estándar de medida utilizada para expresar el valor de bienes y servicios.

Volatilidad: El grado de variación en el precio de un activo a lo largo del tiempo.

Dirección de Billetera: Un identificador único utilizado para enviar y recibir bitcoins en la red Bitcoin, típicamente representado como una cadena de letras y números.

Respaldo de Billetera: Una copia de las claves privadas y la frase de recuperación/palabras semilla de una billetera de Bitcoin, que puede ser utilizada para restaurar el acceso a la billetera en caso de que la original se pierda o sea robada.

Billetera: Un contenedor virtual para bitcoins similar a una billetera física que contiene clave(s) privada(s) que te permiten gastar los bitcoins asignados a ella en la blockchain.

Ballena: Un individuo u organización que posee una cantidad significativa de criptomonedas, capaz de influir en los precios del mercado a través de grandes operaciones.

Hacker Ético (White Hat Hacker): Un hacker ético que utiliza sus habilidades para identificar y solucionar vulnerabilidades en sistemas informáticos y redes.

Libro Blanco (Whitepaper): Un informe que explica el problema y la solución que un proyecto de blockchain o criptomoneda está tratando de abordar.

XBT y BTC: Abreviaturas de bitcoin.

